Talsystemets opbygning

Niss, Mogens Allan

Publication date:
1985

Document Version
Også kaldet Forlagets PDF

Citation for published version (APA):
Niss, M. A. (1985). *Talsystemets opbygning*. Roskilde Universitet. Tekster fra IMFUFA Nr. 100

TEKST NR 100 1985

TALSYSTEMETS OPBYGNING

EN KONSTRUKTIV FREMSTILLING

MOGENS NISS

TEKSTER fra

IMFUFA ROSKILDE UNIVERSITETSCENTER
INSTITUT FOR STUDIET AF MATEMATIK OG FYSIK SAMT DERES FUNKTIONER I UNDERVISNING, FORSKNING OG ANVENDELSER

IMFUFA, Roskilde Universitetscenter, Postboks 26o,
4ooo Roskilde

TATSYSTEMETS OPBYGNING En konstruktiv fremstilling
af MOGENS NISS

IMFUFA tekst nr. loo/1985 296 sider ISSN olo6-6242

Abstract

Teksten præsenterer en konstruktiv fremstilling af talsystemsts opbygning (omfattende talområderne $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$) baseret på et aksiomsystem for de naturlige tal (Peano's aksiomer) og gennemført med et minimum af alment algebraisk apparat. Teksten er udsprunget af og primært rettet til undervisning i emnekredsen "Talsystemets opbygning" i matematikstudiet ved Roskilde Universitetscenter, men vil kunne læses på baggrund af forudsætninger fra den matematisk-fysiske gren i gymnasiet af interesserede.

INDHOLDSFORTEGNELSE side

FORORD

I enhver universitetsuddannelse i matematik er et solidt kendskab til talsystemet og dets delområder, og heriblandt selvfølgelig navnlig de reelle tals område, af grundlæggende betydning. Spørgsmålet er imidlertid hvordan et sådant kendskab bedst opnås. Flere fremgangsmåder står til rådighed. Man kan antage at tidligere undervisning fra folkeskolen og det gymnasiale niveau har givet de studerende så megen fortrolighed med talområderne og deres egenskaber - bortset fra de komplekse tal - at der ikke er behov for at gøre meget mere ved det, med undtagelse måske af at opstille en liste over de træk ved talområderne et universitetsstudium må bygge på. En anden fremgangsmåde er i familje med den nævnte ved ikke at gå nærmere ind på talområdernes frembringelse. Men den adskiller sig fra den ved at anføre et eller andet temmelig kraftigt aksiomsystem, der lader de forskellige talområders karakteristika følge som let erhvervede konsekvenser af de opstillede forudsætninger, for derefter at postulere eksistensen af et sådant system af talområder.

I denne fremstilling er der valgt en tredje vej. Den kan i korthed beskrives ved at sige at alle talområder konstrueres skridtvis ud fra de naturlige tal. Disse er på deres side baseret på et kort, men kraftigt aksiomsystem, der går under navnet Peano's aksiomer. De konstruktionsredskaber der derefter tages i anvendelse hentes fra elementær logik og mængdelære. Det betyder, at de problemer der måtte være ved den udførte konstruktion stammer fra problemer ved dette grundlag, og dér findes som måske bekendt slet ikke så få.

Der kan være gode faglige og pædagogiske grunde for hver af de nævnte fremgangsmåder. Så det er ikke af kanoniske grunde at der for denne fremstilling er valgt den sidstnævnte fremgangsmåde. Snarere skyldes valget mere pragmatiske overvejelser. Den vigtigste af disse er: Ved at vælge det konstruktive approach bliver det muligt at belyse nogle historiske og filosofiske pointer. Forestillingen om en konstruktiv opbygning af talsystemet var central i det sidste århundredes bestræbelser for at skabe et klart og holdbart grundlag for matematikken, eftersom

et sådant grundlag måtte begynde med, eller i det mindste omfatte, talsystemet. Disse bestræbelser havde selvfølgelig mange kilder. En af dem var problemet med tallenes eksistens, hvor både de negative tal, de irrationale tal og de komplekse tal igennem historien havde voldt erkendelsesteoretiske kvaler. Udviklingsarbejdet udført af folk som Cauchy, Bolzano. Hamilton, Weierstrass, Dedekind, Cantor, Méray, Peano, Frege, Weber, Steinitz og Hilbert i løbet af 1800-tallets sidste to tredjedele, kan belyses ved at anskue talsystemet konstruktivt. Udviklingen foregik på et meget frugtbart stadium af matematikkens historie, i omegnen af den gryende mængdelære og dens forjættelser. Man var endnu i bred forstand i det "cantor'ske paradis". Som det vil vides kom der snart slanger i paradis. Der viste sig problemer og paradokser i mængdelæren, som afstedkom en større krise for matematikkens grundlag i gennem de første årtier af dette århundrede. Drømmen om at formalisere sig ud af matematikkens grundlagsspørgsmål brast, om ikke før så med Gödels uafgørlighedssætninger fra begyndelsen af 1930'erne.

I den foreliggende tekst er det logiske grundlag ikke problematiseret. Der er taget udgangspunkt i en naiv mængdelære, hvilket ikke må ses som udtryk for en underkendelse af betydningen af et mere sofistikeret fundament for matematikken, men snarere som et udtryk for det forhold at teksten ikke er en lærebog i logik og mængdelære.

Også en konstruktiv opbygning af tallene kan foretages på forskellige måder, bl.a. med varierende grad af abstrakt algebraisering. I den mest vidtgående almene algebraisering falder talområderne ud som pjuskede specialtilfælde. Jeg har valgt så beskeden en algebraisering som muligt. Dels for at slippe for at opbygge et stort algebraisk apparat af et selvstændigt præg, dels for at komme så tæt som praktisk muligt i en trods alt moderne fremstilling på talområderne "selv". Selvfølgelig kunne der også være pointer i at vælge en vidtgående algebraisk variant, har jeg fundet at omkostningerne overskygger ekstragevinsterne. Alligevel er fremstillingens ramme og sprogbrug nødvendigvis algebraisk. Men apparatet er beskedent, og omfatter stort set kun hvad der er omtalt i appendix-afsnittet "AL-

gebraiske forberedelser".

Tekstens affatning adskiller sig fra det normale. Omkring 1970 fik Anders Madsen og jeg den idé at adskille den teoretiske hovedlandevej i en matematisk tekst fra kommentarer angående idéer og motiver, noter sidebemærkninger, eksempler og illustrationer. Adskillelsen skulle tilvejebringes ved at hovedteksten "i uniform" skulle stå på højresiderne, mens de mereuformelle kommentarer skulle stå på venstresiderne. Dette princip er søgt realiseret i denne tekst. Derved er det muligt, når man først har tilegnet sig stoffet, på et senere tidspunkt at vende tilbage til den tilknappede tekst uden at behøve at læse den pædagogiserende indpakning.

Under arbejdet har jeg ladet mig inspirere af andre fremstillinger. Det drejer sig især om

Svend Bundgaard: TALLENE og Den abstrakte Algebras Grundbegreber, Jul. Gjellerups Forlag, København 1942

H.-D.Ebbinghaus m.fl.: ZAHLEN. Grundwissen Mathematik 1 Springer-Verlag Berlin Heidelberg 1983

W. Fenchel: TALSYSTEMETS OPBYGNING
Købanhavns Universitets Matematiske Institut, 1962-64

Helmuth Gericke: GESCHICHTE DES ZAHLBEGRIFFS
Bibliographisches Institut, Mannheim 1970

E. Mendelson: NUMBER SYSTEMS and the Foundation of Analysis
Academic Press, New York, London 1973

Mogens Niss
8. maj 1985

I. OPBYGNINGEN AF DE NATURLIGE TAL

Uformel indledning

Den indflydelsesrige tyske matematiker Leopold Kronecker, der var virksom i sidste halvdel af det 19. århundrede, er ofte citeret for at have sagt, at Gud skabte de naturlige tal, resten er menneskeværk. Allerede på Kroneckers egen tid var hans præmis udsat for delvis underminering. Richard Dedekind (1831-1916) og Guiseppe Peano (1858-1932) påtog sig en del af skabelsen af de naturlige tal, selv om det selvfølgelig er til genstand for diskussion, hvor råstofferne for skabelsesprocessen er skabt. Dedekinds indsats på dette område findes navnlig i den berømte afhandling "Was sind und was sollen die Zahlen?" (1888). Peanos arbejde er fra 1889. I dette kapitel skal vi præsentere, i en moderne algebraisk ramme, opbygningen af de naturlige tal baseret på Peano's aksiomer, som de kaldes, selv om de i den udformning, hvori de bringes her, rettelig burde tilskrives Dedekind.

Hensigten med opbygningen er at etablere et grundlag, så begrænset og overskueligt som muligt, der er stærkt nok til at tillade tilvejebringelsen af alle de naturlige tals egenskaber, som vi kender dem fra dagligdags omgang med dem. Den intuitive kerne i dette grundlag er for det første efterfølgeroperationen: efter ethvert naturligt tal kommer ét til; processen starter et sted, nemlig med 1, og den kommer aldrig tilbage til et allerede passeret punkt (processen kører ikke i ring). For det andet induktionsprincippet: hvis en mængde M indeholder både 1 og er stabilt over for efterfølgeroperationen (dvs. hver gang et element er med i M, er dets efterfølger det også), er M nødt til at bestå af alle naturlige tal. Dette fører intuitivt frem til at etablere de naturlige tal som (idet efterfølgeroperationen betegnes S): 1, S(1), S(S(1)),...

Et af de filosofiske problemer der ligger bag ønsket om en formel konstruktion af de naturlige tal er, at det ikke er så enkelt at håndtere de prikker, som står efter S(S(1)). Efterfølgerprocessen ender jo aldrig, og vi står derfor aldrig med alle de naturlige tal samlet på én gang. Det er en del af opgaven for den formelle konstruktion at gøre det meningsfuldt at tale om "samlingen af alle naturlige tal" som en helhed, en mængde. Derved bliver de naturlige tals grundlag tæt knyttet til matematikkens grundlag i almindelighed og mængdelærens i særdeleshed. F.eks. spiller klassiske diskussioner om hvad uendelig nærmere er for noget, eller kan bringes til at betyde, ind på dette sted. Disse mere filosofiske problemstillinger skal dog ikke behandles ved denne lejlighed.

Den følgende opbygning af de naturlige tal tager som antydet form af en præcisering og en formalisering af de nævnte intuitive idéer. Denne opbygning er, som det fremgår, baseret på forestillingen om at tælle, fra 1 og fremad i rækkefølge. Det talbegreb der udspringer heraf, kaldes undertiden det ordinale talbegreb. En anden synsmåde repræsenteres af mængdelærens grundlægger Georg Cantor (1845-1918), der hæfter sig ved de naturlige tal som antal. Tallet n anskues her som en prototypemængde, en målestok der repræsenterer alle mængder med n elementer. Dette begreb om de naturlige tal kaldes det kardinale talbegreb, og lægges sædvanligvis ikke til grund for fremstillngen af de naturlige tal. Således heller ikke her. Et par forbindelseslinjer mellem de to talbegreber trækkes dog i slutningen af kapitlet.

Det er vigtigt at gøre sig klart, at vi her forudsætter eksistensen af et system som det beskrevne. Det ligger uden for vores rækkevidde at vise den. Trækkes trådene tilbage til grundlaget i mængdelæren, er eksistensen knyttet til et aksiom om at der findes en uendelig mængde. Denne sag forfølges ikke nøjere her.

Disse aksiomer, der rettelig burde kaldes Dedekinds aksiomer, kaldes ofte for Peano's aksiomer. Overvej hvordan det intuitive indhold af dem svarer til skitsen i den uformelle indledning.

Når vi nu i det følgende gang på gang beviser sætninger, som er indlysende fordi de er kendt fra mange års omgang med naturlige tal, er det vigtigt at fastholde programmet: at opbygge alt hvad der er værd at vide om de naturlige tal alene på grundlag af P1-P3. Derfor er det intetsteds tilladt at benytte betragtninger eller argumenter, som ikke er hentet fra dette grundlag (samt fra logik og mængdelære).

De fleste af de induktionsbeviser, der bringes i denne tekst er lige ud af landevejen, nærmest mekaniske. Prøv i så høj grad som muligt at gennemføre dem selv, inden du læser dem i teksten. Grundmelodien er følgende: Vi vil gerne vise, at en bestemt egenskab E indehaves af alle elementer i $\mathbb{N}$. Til den ende dannes mængden M af alle elementer fra $\mathbb{N}$, der har egenskaben E. Opgaven er så ved induktion at vise, at $M = \mathbb{N}$.

Aksiomsystemet for de naturlige tal. Rekursionssætningen

Vi forestiller os, at der er givet en mængde N, hvori der er fremhævet et element, benævnt u, og hvori der er givet en afbildning $S: N \to N$. Afbildningen S kaldes efterfølgerfunktionen og for $x \in N$ kaldes $S(x)$ efterfølgeren for x.

Lad os antage, at S opfylder følgende egenskaber

P1. $u \notin S(N)$ $(= \{S(x) \mid x \in N\})$

P2. For alle x,y i N gælder:
$x \neq y \Rightarrow S(x) \neq S(y)$ (S er injektiv)

P3. Hvis M er en delmængde af N, som opfylder
(a) $u \in M$
og
(b) For ethvert $x \in M$ vil også $S(x) \in M$,
er $M = N$ (induktionsaksiomet).

I slutningen af kapitlet vil det blive godtgjort, at alle systemer (N,u,S) som opfylder P1-P3, i en bestemt forstand er "ens". Derved er der ingen grund til at skelne mellem dem. Ethvert sådant system vil derfor blive kaldt systemet af naturlige tal. Som fælles betegnelse for et sådant system benytter vi $\mathbb{N}$. I stedet for u skriver vi fra nu af 1.

Alle beviser i dette kapitel beror på afgørende måde på induktion, der jo er den eneste mekanisme som er til rådighed for produktionen af indholdsrige udsagn.

Vi lægger ud med to simple anvendelser af induktionsaksiomet.

Sætning I.1 Om ethvert element $x \in \mathbb{N}$ gælder, at $S(x) \neq x$ (intet objekt er sin egen efterfølger).

Bevis. Vi danner mængden

I følge P1 er 1 ikke en efterfølger. ⟶

Her må grundmelodien modificesres, gennem tilføjelsen af {1}, idet elementet 1 er eksplicit undtaget fra at besidde den egenskab sætningen omhandler. ⟶

$$M = \{x \in \mathbb{N} \mid S(x) \neq x\}.$$

Opgaven er at vise, at $M = \mathbb{N}$. Det sker ved induktion. At M opfylder P3 (a), altså her at $S(1) \neq 1$, følger af at $S(1) \in S(\mathbb{N})$ og $1 \notin S(\mathbb{N})$ (P1).

For at vise, at M opfylder P3 (b), antager vi, at $x \in M$, dvs. at $S(x) \neq x$. I følge P2 må så $S(S(x)) \neq S(x)$. Men det er netop betingelsen for, at $S(x) \in M$. Q.E.D

Sætning I.2. Ethvert $x \in \mathbb{N}$, $x \neq 1$, er en efterfølger, dvs. der findes et $y \in \mathbb{N}$, så at $x = S(y)$.

Bevis. Vi danner mængden

$$M = \{x \in \mathbb{N} \mid \text{der findes et } y \in N, \text{ så at } x = S(y)\} \cup \{1\}$$

Så er det oplagt, at $1 \in M$, hvorved M opfylder P3 (a). For at vise, at M opfylder P3 (b), antager vi, at $x \in M$ og at $x \neq 1$. Altså vil

$$x \in \{x \in \mathbb{N} \mid \text{der findes et } y \in N, \text{ så at } x = S(y)\}.$$

Vi skal godtgøre, at også $S(x) \in M$. Nu angiver

$$\{x \in \mathbb{N} \mid \text{der findes et } y \in \mathbb{N}, \text{ så at } x = S(y)\},$$

som er en delmængde af M, mængden af efterfølgere i $\mathbb{N}$. Da $S(x)$ jo pr. definition er en efterfølger, vil $S(x) \in M$, (som y kan bruges x). Q.E.D.

Det næste skridt i opbygningen er etableringen af en generel mekanisme, der tillader os at indføre forskellige algebraiske og andre operationer i de naturlige tal. Dette sker gennem en nøglesætning, som ganske vist kræver et lidt omstændeligt bevis, men som derefter reducerer den resterende opbygning til en lang række overskuelige anvendelser af sætningen.

Det er nok en god idé at betragte et eksempel på hvad sætninger siger, inden man kaster sig over beviset. Vi lader som om vi kender de reelle tal $\mathbb{R}$. Lad $A = \mathbb{R}$, $a \in \mathbb{R}$ være givet, og $g:\mathbb{R} \sim \mathbb{R}$ være defineret ved $g(z) = az$ for $z \in \mathbb{R}$. Så fortæller sætningen, at der findes en funktion $F: \mathbb{N} \sim \mathbb{R}$, så at

$$F(1) = a \text{ og } F(x+1) = F(S(x)) = g(F(x)) = aF(x),$$

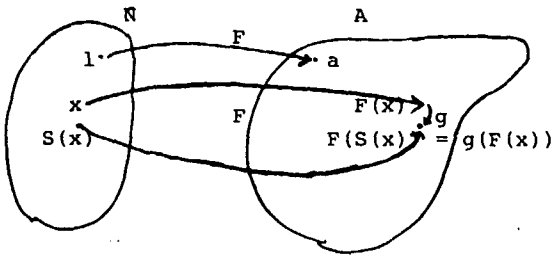
dvs. $F(1) = a$, $F(2) = aF(1) = a \cdot a$ $(= a^2)$, $F(3) = aF(2) = a \cdot (a \cdot a)$ $(= a^3)$, osv.

Sætningen giver altså en rekursiv definition af potenserne a^n efter skemaet:

$$a^1 = a,\ a^2 = a \cdot a, .., a^{n+1} = a \cdot a^n, ... \text{osv.}$$

Med indførelsen af addition og multiplikation efter Sætning I.4. og Sætning I.9. gives andre eksempler på hvad sætningen udsiger.

Illustration til sætningen:



Hovedidéen i eksistensdelen af beviset er at konstruere den søgte funktion F defineret på hele $\mathbb{N}$ ved først at skabe funktioner, der ligner den søgte hvad egenskaber angår, men som hver for sig kun er defineret på en mængde indeholdende de naturlige tal "fra 1 til n". Derefter indfanges ethvert naturligt tal x af definitionsmængden for en sådan funktion f. Og F's værdi i x defineres så til at være $F(x) = f(x)$. Dette kræver, at uanset hvilken af de mulige f-funktioner vi vælger, bliver værdien f(x) den samme.

Grunden til at konstruktionen bliver omstændelig, er, at vi på det indtil nu foreliggende grundlag ikke er i stand til at tale om de naturlige tal "fra 1 til n" på en præcis og meningsfuld måde. Det ville nemlig forudsætte, at vi havde tillagt "fra" og "til" mening inden for de naturlige tal, hvilket i realiteten først kan gøres med rekursionssætningens resultater til rådighed. T1-T3 udtrykker intuitivt, at alle tal "fra 1 og til og med n" er med i M, og at M hænger sammen fra top til bund.

Sætning I.3. (Rekursionssætningen) Lad A være en vilkårlig (ikke-tom) mængde, og lad $a \in A$ være givet. Antag endvidere, at der er givet en afbildning $g: A \sim A$.
Så findes én og kun én funktion $F:\mathbb{N} \sim A$, som opfylder:
(1) $F(1) = a$
og
(2) $F(S(x)) = g(F(x))$ for alle $x \in \mathbb{N}$.

Bevis. Sætningen, der skyldes Dedekind (1888), indedholder både en eksistens- og en entydighedspåstand. Først entydigheden:

Lad os antage, at der var to funktioner F_1 og F_2, som begge opfyldte (1) og (2). Vi vil vise, at de er identiske. Til den ende sættes

$$M = \{x \in \mathbb{N} \mid F_1(x) = F_2(x)\}.$$

Kan vi vise, at $M = \mathbb{N}$, har vi godtgjort, at $F_1 = F_2$. At $1 \in M$, følger nu af at $F_1(1) = a = F_2(1)$. Er dernæst $x \in M$, må S(x) også tilhøre M, thi

$$F_1(S(x)) = g(F_1(x)) = g(F_2(x)) = F_2(S(x)),$$

hvor de to yderste lighedstegn blot er betingelsen (2), mens det midterste lighedstegn følger af, at $F_1(x) = F_2(x)$ (fordi $x \in M$). Derved opfylder M både P3 (a) og P3 (b), således at $M = \mathbb{N}$.

Dernæst eksistensen, som repræsenterer besværet:

Lad $n \in \mathbb{N}$. En afbildning f defineret på en delmængde M af N med værdier i A, $f: M \sim A$, kaldes n-tilgængelig, hvis

T1. $1 \in M$
T2. $n \in M$
P3. For alle $x \in \mathbb{N}$ gælder, at hvis $S(x) \in M$ vil $x \in M$

(betingelser vedrørende M)
og
T4. $f(1) = a$
T5. For ethvert $x \in \mathbb{N}$ gælder:
$S(x) \in M \Rightarrow f(S(x)) = g(f(x))$
(betingelser vedrørende f)

Eksistenbeviset forløber nu i fire skridt.

Intuitivt udsiger (A) blot, at hvis f opfylder tilgængelighedsbetingelsen på $\{1,\ldots,n,S(n)\}$ (som vi altså endnu ikke kan tale om på denne måde), da også på $\{1,\ldots,n\}$, som jo er en delmængde heraf (og som vi heller ikke kan tale om endnu).

(A). Hvis f er S(n)-tilgængelig, er f også n-tilgængelig. Alle betingelserne på nær T2. er de samme for S(n)-tilgængelighed som for n-tilgængelighed, idet de ikke afhænger af n. Det eneste, vi mangler for at vise, at f er n-tilgængelig, er altså T2: $n \in M$. Da $S(n) \in M$ (fordi f er S(n)-tilgængelig), følger imidlertid af T3., at $n \in M$, hvilket er det ønskede.

Idéen i (B) er (stadig intuitivt) at starte med at fastlægge en 1-tilgængelig funktion $f_1: M_1(\supseteq\{1\}) \rightsquigarrow A$. Derefter fastlægges en 2-tilgængelig funktion $f_2: M_2(\supseteq\{1,2\}) \rightsquigarrow A$, og så fremdeles, en n-tilgængelig funktion

$$f_n: M_n(\supseteq\{1,2,\ldots n\}) \rightsquigarrow A.$$

Det kommer så til at gælde, at hver funktion f_n er en udvidelse af den foregående. Læg stadig mærke til, at vi ikke formelt kan tale om mængder som $\{1,2,\ldots n\}$.

(B). For ethvert $n \in \mathbb{N}$ eksisterer en n-tilgængelig funktion. Dette bevises ved induktion. Vi sætter

$$P = \{n \in \mathbb{N} \mid \text{der findes mindst én n-tilgængelig funktion}\}$$

Vi vil vise, at P opfylder P3 (a) og (b). At P opfylder P3 (a), dvs. $1 \in P$, følger da $M = \{1\}$ og $f(1) = a$ åbenbart bestemmer en 1-tilgængelig funktion. Betingelserne T3 og T5 er opfyldt, fordi der ikke findes noget $S(x) \in M$, når $M = \{1\}$ (P1). Lad nu $n \in P$, dvs. der findes en n-tilgængelig funktion $f: M \rightsquigarrow A$, vil vi konstruere en S(n)-tilgængelig funktion f^*.

Først sættes $M^* = M \cup \{S(n)\}$. For $x \in M$ sættes $f^*(x) = f(x)$. For $x = S(n)$ sættes $f^*(S(n)) = g(f(n))$. Det skal nu blot checkes, at $f^*: M^* \rightsquigarrow A$ er S(n)-tilgængelig; så har vi konstrueret en S(n)-tilgængelig funktion, og induktionen er gennemført. At $1 \in M^*$, $S(n) \in M^*$, $f^*(1) = a$, som netop er betingelserne T1, T2 og T4, er oplagt. Hvis dernæst - med henblik på T3 - $S(x) \in M^* = M \cup \{S(n)\}$, vil enten $S(x) \in M$, og dermed (da f er n-tilgængelig) $x \in M$, eller $S(x) = S(n)$, og dermed $x = n \in M$, p.g.a. P2. Dette viser, at betingelse T3 er opfyldt. Tilbage står at vise betingelse T5.

(C) godtgør, at der er ligegyldigt, hvilken n-tilgængelig funktion vi vælger, når værdien af F på n skal fastlægges. Dette skridt er nødvendigt for at sikre utvetydighed i definitionen F(n) = f(n).

I (D) skummes blot fløden af det foregående. Det er uden dybsindigheder at eftervise, at F har de ønskede egenskaber.

Hvis $S(x) \in M^* = M \cup \{S(n)\}$, vil igen enten $S(x) \in M$, hvorved

$$f^*(S(x)) = f(S(x)) = g(f(x)) = g(f^*(x))$$

(det midterste lighedstegn følger af, at f er n-tilgængelig), eller $S(x) = S(n)$, hvorved pr. definition af f^* og da $x = n$:

$$f^*(S(x)) = f^*(S(n)) = g(f(n)) = g(f^*(n)) = g(f^*(x)).$$

Vi har nu godtgjort, at f^* er S(n)-tilgængelig, og dermed at $S(n) \in P$. I alt opfylder P så P3 (a) og (b), således at $P = \mathbb{N}$.

(C) Hvis f og h begge er n-tilgængelige, er $f(n) = h(n)$. Også dette skal bevises ved induktion. Lad

$$Q = \{n \in \mathbb{N} \mid \text{For alle funktioner f og h gælder, at hvis f og h er n-tilgængelige, så er } f(n) = h(n)\} .$$

Vi skal vise, at Q opfylder P3 (a) og P3 (b). At $1 \in Q$, følger af, at hvis $f: M_1 \sim A$ er 1-tilgængelig og $h: M_2 \sim A$ også er 1-tilgængelig, vil $f(1) = a = h(1)$, således, at $f(1) = h(1)$.

Lad dernæst $n \in Q$. Opgaven er så at vise, at $S(n) \in Q$. Hvis f og h er to vilkårlige S(n)-tilgængelige funktioner, er de i følge (A) også n-tilgængelige. Da $n \in Q$, er så $f(n) = h(n)$. Videre er

$$f(S(n)) = g(f(n)) = g(h(n)) = h(S(n)).$$

Men det viser, at $S(n) \in Q$, hvorved induktionsbeviset for (C) er gennemført.

(D) Konstruktionen af den søgte funktion F.
Lad $n \in \mathbb{N}$. Så findes i følge (B) en n-tilgængelig funktion f. Vi sætter nu

Man kunne måske få den tanke, at vi her (og i punkt B) i beviset kommer til at udføre konstruktioner af netop den art sætningen skal tillade os at udføre, at altså foretagendet kører i ring. Sådan forholder det sig imidlertid ikke. Sætningen påstår eksistensen af en bestemt slags rekursivt fastlagt funktion F på hele $\mathbb{N}$. Vi konstruerer denne funktion ved at løse den "ufarlige" opgave først at konstruere en skare af beslægtede funktioner, én på hvert endeligt afsnit af $\mathbb{N}$, for derefter at definere F eksplicit, altså ikke rekursivt, ud fra værdien af de "ufarlige" funktioner.

Det intuitive indhold er, at vi for m fast definerer addition af m til n rekursivt (tilbageløbende) ved: m lagt til 1 skal være S(m), og: hvis vi ved hvad m lagt til n skal betyde, skal m lagt til n+1 (S(n)) betyde det foregående plus 1. Altså m+1 = S(m), m+(n+1) = (m+n)+1, som netop er (5) og (7) nedenfor. Den intuitive tolkning af, hvad F_m gør ved n er "læg m til n".

$$F(n) = f(n) \quad (\in A),$$

hvilket giver mening, da vi får samme værdi, uanset hvilken n-tilgængelig funktion f vi vælger (C). Dermed har vi defineret $F: \mathbb{N} \sim A$, og mangler blot at indse, at F har de krævede egenskaber:

$$F(1) = f(1) = a$$

for en(hver)1-tilgængelig funktion f. Dette giver sætningens betingelse (1).

Hvad angår betingelse (2), har vi:

$$F(S(n)) = f(S(n))$$

for en(hver) S(n)-tilgængelig funktion f. Da f er S(n)-tilgængelig, vil S(n) tilhøre definitionsmængden for f, hvorved (p.g.a. T5):

$$f(S(n)) = g(f(n)) = g(F(n)).$$

Men så er i alt:

$$F(S(n)) = g(F(n)),$$

hvilket er betingelse (2) for F.

Hermed er beviset for sætningen fuldført. Q.E.D.

Indførelse af addition i de naturlige tal

Med rekursionssætningen til rådighed er vi nu i stand til at indføre kompositionen addition i de naturlige tal. Dette sker ved hjælp af

Sætning I.4. Lad $m \in \mathbb{N}$. Så findes en entydigt bestemt funktion $F_m: \mathbb{N} \sim \mathbb{N}$, så at

(3) $F_m(1) = S(m)$

(4) $F_m(S(n)) = S(F_m(n))$ for alle $n \in \mathbb{N}$.

Pas på ikke at blive forledt til at tro, at $m + n = n + m$. Rækkefølgen af m og n i $m + n$ betyder noget, nemlig F_m's værdi på n. Det er principielt noget andet end $n + m$, der er F_n's værdi på m. At der imidlertid faktisk er identitet mellem de to kræver et bevis (se Sætning I.6.).

Indholdet af Sætning I.5. er i virkeligheden mindre trivielt end det ser ud til. Sætningen siger nemlig, at

$$F_x(y+z) = F_{x+y}(z), \text{ for alle } x,y,z \text{ i } \mathbb{N},$$

altså at enhver F_x-funktions virkning på $(y+z)$ giver samme resultat som enhver F_{x+y}-funktions virkning på z. Når bevi-set alligevel forløber uden problemer, er det fordi betingelsen (7) er et specialtilfælde af associativiteten, idet denne fremgår af (7) ved at erstatte 1 med et hvilketsomhelst naturligt tal.

Læg mærke til, at når x og y, som er vilkårlige, fastholdes, bliver udsagnet i sætningen, at $x + (y + z) = (x + y) + z$ gælder for alle z.

Bevis: Påstanden følger som et specialtilfælde af rekursionssætningen med $A = \mathbb{N}$, $a = S(m)$ og $g = S$. Q.E.D.

Vi indfører nu kompositionen + ved:

Definition: $m + n = F_m(n)$ for alle $m,n \in \mathbb{N}$.

Betingelserne (3) og (4) kan så udtrykkes

(5) $m + 1 = S(m)$ for alle $m \in \mathbb{N}$
(6) $m + S(n) = S(m+n)$ for alle $m,n \in \mathbb{N}$

Vi kan omskrive (6) ved hjælp af (5):

(7) $m + (n + 1) = (m + n) + 1$ for alle $m,n \in \mathbb{N}$

På dette grundlag kan egenskaberne ved addition opnås. Disse egenskaber indeholdes i de følgende sætninger.

> Sætning I.5. (Associativitet af addition) For alle $x,y,z \in \mathbb{N}$ gælder, at
> $x + (y + z) = (x + y) + z$.

Bevis: Lad x og y være vilkårlige naturlige tal. Vi sætter nu

$$M_{xy} = \{z \in \mathbb{N} \mid x + (y + z) = (x + y) + z\}$$

og vil ved induktion indse, at $M_{xy} = \mathbb{N}$, hvilket vil fuldføre beviset.

At $1 \in M_{xy}$, dvs. at $x + (y + 1) = (x + y) + 1$, er simpelthen (7). Vi mangler derfor blot at vise, at hvis $z \in M_{xy}$ så vil også $S(z)$ $(= z + 1)$ også tilhøre M_{xy}. Men

$$x + (y + S(z)) = x + (S(y+z)) = S(x + (y + z))$$
$$= S((x + y) + z) = (x + y) + S(z),$$

hvor alle lighedstegn, på nær det tredje, fremkommer ved anvendelse af (6), mens det tredje skyldes antagelsen $z \in M_{xy}$. I alt har vi opnået, at $S(z) \in M_{xy}$. Q.E.D.

Sætning I.6. (Kommutativitet af addition). For alle $x, y \in \mathbb{N}$ gælder, at
$x + y = y + x$.

Det kan måske forekomme overraskende, at denne sætning er besværligere at bevise end den foregående. Det skyldes imidlertid, at der ikke i rekursionssætningen indgår noget indbygget specialtilfælde af kommutativitet, i modsætning til hvad tilfældet var for associativitet. Kernen i beviset bliver derved at indse, at $x + 1 = 1 + x$ for alle x i $\mathbb{N}$, og det bliver i realiteten en lille sætning for sig at bevise. Dette sker i det væsentlige ved hjælp af associativiteten (og, naturligvis, efterfølgerfunktionens egenskaber).

Bevis: Beviset føres som et induktionsbevis. Lad $x \in \mathbb{N}$ være vilkårligt valgt. Nu dannes

$$M_x = \{y \in \mathbb{N} \mid x + y = y + x\}$$

Det skal vises, at M_x opfylder P3 (a) og (b). Vi viser først, at $1 \in M_x$, dvs. at $x + 1 = 1 + x$. Dette sker ved et selvstændigt induktionsbevis, idet vi sætter

$$M = \{x \in \mathbb{N} \mid x + 1 = 1 + x\} .$$

At $1 \in M$ kommer ud på, at $1 + 1 = 1 + 1$, hvilket er en oplagt konsekvens af, at de to sider af lighedstegnet simpelthen er identiske. Hvis dernæst $x \in M$, vil også $S(x) \in M$, thi

$$S(x) + 1 = (x + 1) + 1 = (1 + x) + 1 = 1 + (x + 1)$$
$$= 1 + S(x).$$

De to yderste lighedstegn kommer af (6), det andet af induktionsforudsætningen $x \in M$, det tredje af associativiteten. Dermed er det vist, at M_x opfylder P3 (a).

For at vise, at M_x opfylder P3 (b) betragtes et vilkårligt $y \in M_x$. Vi skal indse, at $S(y) \in M_x$. Men

$$x + S(y) = S(x+y) = S(y+x) = (y + x) + 1$$
$$= y + (x + 1) = y + (1 + x) = (y + 1) + x$$
$$= S(y) + x.$$

Den omvendte sætning til forkortningsreglen : hvis x = y er x + z = y + z, er selvfølgelig trivielt opfyldt, idet de to sider i identiteten x + z = y + z, jo simpelthen får nøjagtig samme form.

Denne sætning fortæller, at addition aldrig fører tilbage til udgangspunktet.

Her skyldes det første lighedstegn (6), det andet induktionsforudsætningen $y \in M_x$, det tredje (5), det fjerde associativiteten, det femte, at $1 \in M_x$, det sjette associativiteten, det sidste (5). Hermed er sætningen bevist. Q.E.D .

Sætning. I.7. (Forkortningsreglerne for addition): For alle $x,y,z \in \mathbb{N}$ gælder, at hvis
$x + z = y + z$
er $x = y$.

Bevis: Lad x og y være vilkårlige naturlige tal. Sættes

$$M_{xy} = \{z \in \mathbb{N} \mid x + z = y + z \Rightarrow x = y\}$$

vil vi ved induktion indse, at $M_{xy} = \mathbb{N}$.

At $1 \in M_{xy}$ følger således: Hvis $x + 1 = y + 1$, vil $S(x) = S(y)$ (p.g.a. (5)), og dermed $x = y$, i kraft af P2.

Lad dernæst $z \in M_{xy}$, dvs. hvis $x + z = y + z$ er $x = y$. Det skal godtgøres, at $S(z) \in M_{xy}$, dvs. hvis $x + S(z) = y + S(z)$ må $x = y$. Men af $x + S(z) = y + S(z)$ følger af (6), at $S(x+z) = S(y+z)$, hvorfor $x + z = y + z$ (p.g.a. P2). Men dette afstedkommer, idet $z \in M_{xy}$, at $x = y$. Q.E.D.

Sætning I.8. For alle $x,y \in \mathbb{N}$ gælder, at
$x + y \neq x$.

Bevis: Lad $x \in \mathbb{N}$. Så sættes

$$M_y = \{x \in \mathbb{N} \mid x + y \neq x\}.$$

Det vil blive vist ved induktion, at $M_y = \mathbb{N}$.

At $1 \in M_y$, altså at $1 + y \neq 1$, følger af, at $1 + y = S(y) \neq 1$,

Det intuitive indhold er, at vi for m fast definerer multiplikation med m rekursivt ved: m gange 1 skal betyde m. Hvis vi ved hvad m gange n skal betyde, definerer vi m gange n+1 (= S(n)) til at betyde "m gange n , plus m", idet vi efter indførelsen af addition godt ved, hvad addition af m skal betyde. Altså $m\cdot 1 = m$, $m(1+1) = m\cdot 1+m = m+m$, $m\cdot((1+1)+1) = m\cdot(1+1)+m = (m+m)+m$, eller generelt: $m\cdot 1 = m$, $m\cdot(n+1) = m\cdot n+m$, som netop er (1o) og (11) nedenfor. Den intuitive tolkning af hvad G_m gør ved n er "gang n med m".

Pas også her på ikke umiddelbart at tro,at operationen er kommutativ, altså at $m\cdot n = n\cdot m$. De er principielt forskellige, idet $m\cdot n = G_m(n)$ og $n\cdot m = G_n(m)$. At der imidlertid faktisk er identitet følger af Sætning O.11.

(1o) kan også udtrykkes "1 er højre-neutralt ved ·". At 1 også er venstre-neutralt følger når kommutativiteten er vist (Sætning I.11.)

Når vi med Sætning I.11 har indset, at · er kommutativ, er de to identiteter ens. Men dette resultat står altså endnu ikke til rådighed. Beviset for det benytter faktisk distributiviteten.

Læg i øvrigt mærke til, at (11) er et specialtilfælde af distributiviteten, der i sin generelle form fremkommer ved at erstatte 1 med et vilkårligt naturligt tal. Derfor bliver beviset simpelt.

($1 \notin S(\mathbb{N})$, P1). Er dernæst $x \in M_y$,dvs. $x + y \neq x$, vil også $S(x) \in M_y$. Thi

$$S(x) + y = S(x+y) \neq S(x),$$

hvor forskelligheden skyldes, at $x + y \neq x$ (P2). Men så er beviset fuldført . Q.E.D.

Indførelse af multiplikation i de naturlige tal

Også multiplikation i de naturlige tal indføres ved hjælp af rekursionssætningen.

> Sætning I.9. Lad $m \in \mathbb{N}$. Så findes en entydigt bestemt funktion $G_m: \mathbb{N} \sim \mathbb{N}$, så at
> (8) $G_m(1) = m$
> (9) $G_m(S(n)) = F_m(G_m(n))$ $(= G_m(n) + m)$ for alle $m,n \in \mathbb{N}$

Bevis: Påstanden følger som et specieltilfælde af rekursionssætningen med $A = \mathbb{N}$, $a = m$ og $g = F_m$. Q.E.D.

Vi indfører nu kompositionen · ved

Definition: $m\cdot n = G_m(n)$ for alle $m,n \in \mathbb{N}$.

Betingelserne (8) og (9) kan så skrives

(1o) $m\cdot 1 = m$, for alle $m \in \mathbb{N}$
(11) $m\cdot(n + 1) = m\cdot n + m$, for alle $m,n \in \mathbb{N}$.

I stedet for $m\cdot n$ skrives ofte mn.

Egenskaberne ved multiplikation fremgår af de følgende sætninger.

> Sætning I.1o. (Distributivitet): For alle x,y,z i $\mathbb{N}$ gælder, at
> $x\cdot(y + z) = x\cdot y + x\cdot z$ og at
> $(y + z)\cdot x = y\cdot x + z\cdot x$

Bevis: Vi deler beviset i to dele, én for hver identitet. Først den første:

Lad x og y være vilkårlige naturlige tal. Så sættes

$$M_{xy} = \{z \in \mathbb{N} \mid x\cdot(y+z) = x\cdot y + x\cdot z\}$$

Ved induktion vil vi bevise, at $M_{xy} = \mathbb{N}$. At $1 \in M_{xy}$, altså at $x\cdot(y + 1) = x\cdot y + x\cdot 1$, fås på denne måde:

$$x\cdot(y + 1) = x\cdot y + x = x\cdot y + x\cdot 1$$

idet det første lighedstegn er (11), det andet (1o).

Er dernæst $z \in M_{xy}$, skal det godtgøres, at $S(z) \in M_{xy}$. Men

$$x\cdot(y + S(z)) = x\cdot(S(y+z)) = x\cdot((y + z) + 1)$$
$$= x\cdot(y + z) + x = (x\cdot y + x\cdot z) + x$$
$$= x\cdot y + (x\cdot z + x) = x\cdot y + x\cdot(z + 1) = x\cdot y + x\cdot S(z),$$

hvor de enkelte lighedstegn,i rækkefølge, skyldes henholdsvis: (6),(5),(11), induktionsforudsætningen $z \in M_{xy}$, associativiteten af +, (11) og (5). Dermed er induktionsbeviset for den første identitet gennemført.

Den anden identitet bevises på samme måde:

Lad $y,z \in \mathbb{N}$ være vilkårlige. Vi danner

$$M_{yz} = \{x \in \mathbb{N} \mid (y + z)\cdot x = y\cdot x + z\cdot x\}$$

og beviser ved induktion, at $M_{yz} = \mathbb{N}$.

At $1 \in M_{yz}$, altså at $(y + z)\cdot 1 = y\cdot 1 + z\cdot 1$,fås således:

$$(y + z)\cdot 1 = y + z = y\cdot 1 + z\cdot 1$$

ved gentagen anvendelse af (1o).

Ligesom tilfældet var med kommutativiteten af +, er det her først nødvendigt at bevise, at x og 1 kommuterer. Hvor beviset for + essentielt beroede på associativiteten, beror det her på distributiviteten.

Er dernæst $x \in M_{yz}$, dvs. er $(y + z)\cdot x = y\cdot x + z\cdot x$, må vi eftervise, at $S(x) \in M_{yz}$. Men

$$(y + z)\cdot S(x) = (y + z)\cdot(x + 1) = (y + z)\cdot x + (y + z)$$
$$= (y\cdot x + z\cdot x) + (y + z) = (y\cdot x + y) + (z\cdot x + z)$$
$$= y\cdot(x + 1) + z\cdot(x + 1) = y\cdot S(x) + z\cdot S(x).$$

I rækkefølge begrundes lighedstegnene af: (5), (11), induktionsforudsætningen $x \in M_{yz}$, associativiteten af +, dobbelt anvendelse af (11), samt til slut dobbelt anvendelse af (5). Hermed er også den anden identitet bevist. Q.E.D.

Sætning I.11. (Kommutativitet af multiplikation): For alle $x,y \in \mathbb{N}$ gælder, at
$x\cdot y = y\cdot x$.

Bevis: Beviset føres undtagelsesvis ved induktion.

Lad $x \in \mathbb{N}$ være vilkårligt valgt. Så dannes

$$M_x = \{y \in \mathbb{N} \mid x\cdot y = y\cdot x\}$$

Det bevises først ved et selvstændigt induktionsbevis, at $1 \in M_x$. Vi sætter

$$M = \{x \in \mathbb{N} \mid x\cdot 1 = 1\cdot x\}$$

At $1 \in M$, altså at $1\cdot 1 = 1\cdot 1$, kommer af, at de to sider af lighedstegnet er identiske. Hvis dernæst $x \in M$, dvs. $x\cdot 1 = 1\cdot x$, må også $S(x) \in M$. Thi

$$S(x)\cdot 1 = S(x) = x + 1 = x\cdot 1 + 1 = 1\cdot x + 1 = 1\cdot(x+1) = 1\cdot S(x),$$

resulterende af henholdsvis (1o), (5), (1o), induktionsforudsætningen $x \in M$, og endelig (11).

Dermed har vi bevist, at $1 \in M_x$.

Dette er ikke et induktionsbevis! 

Vi mangler at vise, at hvis $y \in M_x$, dvs. hvis $x \cdot y = y \cdot x$, vil også $S(y) \in M_x$. Til den ende noterer vi, at

$$x \cdot S(y) = x \cdot y + x = y \cdot x + x = y \cdot x + 1 \cdot x = (y + 1) \cdot x = S(y) \cdot x,$$

hvor det første lighedstegn følger af (11), det andet af induktionsantagelsen $y \in M_x$, det tredje af (1o) og af at $1 \in M_x$, det fjerde af distributiviteten, det sidste af (5). Vi har fundet, at $S(y) \in M_x$, og beviset er fuldført. Q.E.D.

Sætning I.12. (Associativitet af multiplikation): For alle $x,y,z \in \mathbb{N}$ gælder, at $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Bevis: Lad $x,y \in \mathbb{N}$ være vilkårlige. Så defineres

$$M_{xy} = \{z \in \mathbb{N} \mid x \cdot (y \cdot z) = (x \cdot y) \cdot z\}$$

Ved induktion vil vi godtgøre, at $M_{xy} = \mathbb{N}$.

At $1 \in M_{xy}$, altså at $x \cdot (y \cdot 1) = (x \cdot y) \cdot 1$, ses således:

$$x \cdot (y \cdot 1) = x \cdot y = (x \cdot y) \cdot 1$$

med dobbelt anvendelse af (1o).

Hvis $z \in M_{xy}$, altså $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, vil også $S(z) \in M_{xy}$, fordi

$$x \cdot (y \cdot S(z)) = x \cdot (y \cdot (z + 1)) = x \cdot (y \cdot z + y) = x \cdot (y \cdot z) + x \cdot y = (x \cdot y) \cdot z + x \cdot y = (x \cdot y) \cdot z + (x.y) \cdot 1 = (x \cdot y) \cdot (z + 1) = (x \cdot y) \cdot S(z),$$

på grund af henholdsvis (5), (11), distribitivitet, induktionsforudsætningen $z \in M_{xy}$ (1o), distributivitet samt

Også her er den omvendte sætning triviel: Hvis x = y, er x·z = y·z for ethvert z, fordi x·z og y·z simpelthen har identisk form, når x = y.

Til forskel fra de fleste andre induktionsbeviser, vi har ført i dette afsnit, fastholdes her ikke to af de involverede elementer. I stedet er her induktionsegenskaben for y:'For alle x,z gælder: hvis...så'

Læg i øvrigt i beviset mærke til, at det er lidt mindre ud af landevejen, end de andre induktionsbeviser. Det skyldes, at vi ikke straks på basis af x·z = S(y)·z (= y·z+z) kan benytte induktionsforudsætningen y ∈ M. Det er nødvendigt at skelne mellem om x = 1 eller x ≠ 1 (og benytte, at x i det sidste tilfælde er en efterfølger), for at bringe denne forudsætning i spil.

Med denne sætning er indførelsen af addition og multiplikation i ℕ og kortlægningen af deres vigtigste algebraiske egenskaber tilendebragt. Vi kan nu frit, dvs. som vi plejer, operere med udtryk involverende + og ·.

sluttelig (5). I alt har vi indset, at S(z) ∈ M_{xy}·Q.E.D.

Sætning I.13. (Forkortningsreglerne for multiplikation): For alle x,y,z ∈ ℕ gælder, at
hvis x·z = y·z,
er x = y. Tilsvarende hvis z·x = z·y.

Bevis: Beviset føres ved induktion. Vi danner

$$M = \{y \in \mathbb{N} \mid \text{For vilkårlige } x,z \in \mathbb{N} \text{ gælder: } x\cdot z = y\cdot z \Rightarrow x = y\}$$

Vi vil vise, at M = ℕ.

Først bevises, at 1 ∈ M, altså at for vilkårlige x,z ∈ ℕ for hvilke x·z = 1·z, må x = 1. Lad altså x,z ∈ ℕ opfylde, at x·z = 1·z. Var nu x ≠ 1, ville x være en efterfølger (Sætning I.2.): x = S(u) for et eller andet u ∈ ℕ. Så ville S(u)·z = x·z = 1·z = z, og dermed, da S(u) = u+1,

$$u\cdot z + z = (u + 1)\cdot z = z$$

i strid med Sætning I.8. Vi slutter derfor, at x = 1.

Dernæst skal det indses, at hvis y ∈ M, vil også S(y) ∈ M. Dette kommer ud på at vise, at hvis x·z = S(y)·z må x = S(y), uanset hvilke x,z der er tale om. Det antages altså, at x·z = S(y)·z. Heraf finder vi, at

$$x\cdot z = S(y)\cdot z = (y + 1)\cdot z = y\cdot z + z.$$

Men så må x ≠ 1. Var nemlig x = 1, ville z = y·z + z, i strid med Sætning I.8. Da altså x ≠ 1, er x i følge Sætning I.2. en efterfølger: x = S(u). Deraf får vi, at

$$u\cdot z + z = (u + 1)\cdot z = S(u)\cdot z = x\cdot z = y\cdot z + z.$$

Ved hjælp af forkortningsreglerne for addition slutter vi, at u·z = y·z. Men da y ∈ M, følger at u = y, og dermed, at x = S(u) = S(y). Q.E.D.

Relationen < er på dette sted principielt ukendt. Indførelsen af den sker altså via addition. Den sammenhæng, der fremhæves i definitionen er velkendt fra "dagligdagens omgang" med de naturlige tal.

(12), (13) og (14) kan også udtrykkes: Hvis $x \neq y$ har netop én af ligningerne $x + z = y$ og $y + z = x$ en løsning i z.

Ordning i de naturlige tal

Ordningen i de naturlige tal indføres på grundlag af additionen.

Definition: For $x,y \in \mathbb{N}$ skrives $x < y$ hvis og kun hvis der findes et $z \in \mathbb{N}$, så at $x + z = y$.

Vi skriver $x \not< y$ for $\neg(x < y)$ og $x > y$ for $y < x$.

Egenskaberne ved relationen < kommer til udtryk i en række sætninger.

Sætning I.14. For vilkårlige $x,y \in \mathbb{N}$ gælder enten (12), (13) eller (14), men ikke to af dem samtidig:
(12) $x = y$
(13) der findes netop ét $z \in \mathbb{N}$, så at $x + z = y$
(14) der findes netop ét $z \in \mathbb{N}$, så at $y + z = x$.
Endvidere: (13) gælder hvis og kun hvis $x < y$; (14) gælder hvis og kun hvis $y < x$.

Bevis: Lad y være et vilkårligt naturligt tal. Så sættes

$$M_y = \{x \in \mathbb{N} \mid \exists\, z \in \mathbb{N}: x + z = y\} \cup \{x \in \mathbb{N} \mid \exists\, z \in \mathbb{N}: y + z = x\} \cup \{y\}$$

$$= A \cup B \cup \{y\}.$$

Vi vil vise ved induktion, at $M_y = \mathbb{N}$.

At $1 \in M_y$ indses således: Hvis $1 = y$, vil $1 \in \{y\} \subseteq M_y$. Hvis $1 \neq y$, er y en efterfølger (Sætning I.2.), dvs. der findes et $z \in \mathbb{N}$, så at $y = S(z)$. Men så vil $1 + z = S(z) = y$, hvorved $1 \in A \subseteq M_y$.

Antages dernæst, at $x \in M_y$ skal vi vise, at også $S(x) \in M_y$. Antagelsen $x \in M_y$ er ensbetydende med, at enten vil $x \in A$, $x \in B$ eller $x \in \{y\}$. Hvis $x \in A$ findes $z \in \mathbb{N}$, så at $x + z = y$. Er her $z = 1$, vil $S(x) = x + 1 = y$, dvs. $S(x) \in \{y\} \subseteq M_y$.

Er derimod $z \neq 1$, er z en efterfølger (Sætning I.2.), $z = S(u)$, hvorved $y = x + S(u) = S(x+u) = S(x) + u$, så at $S(x) \in A \subseteq M_y$. Hvis $x \in B$, findes et $z \in \mathbb{N}$, så at $y + z = x$, hvorved $y + S(z) = S(y+z) = S(x)$, således at $S(x) \in B \subseteq M_y$. Hvis endelig, som den tredje mulighed, $x \in \{y\}$, dvs. $x = y$, er $S(x) = S(y) = y + 1$, dvs. $S(x) \in B \subseteq M_y$. I alle tilfælde har vi fundet, at $S(x) \in M_y$. Hermed er bevist, at $M_y = \mathbb{N}$.

Hvis der findes et $z \in \mathbb{N}$, så at $x + z = y$, findes der kun det samme. Thi $x + u = y$ og $x + z = y$ bevirker, at $x + u = x + z$, hvorefter forkortningsreglerne for addition giver, at $z = u$. Dette retfærdiggør ordet "netop" i formuleringen af (13). Tilsvarende for (14).

At (12), (13) og (14) to og to er gensidigt udelukkende ses således:
(12) og (13) udelukker hinanden, fordi $x = y$ og $x + z = y$ ville føre til $x + z = x$ i strid med Sætning I.8.
(12) og (14) udelukker på samme måde hinanden, fordi $x = y$ og $y + z = x$ giver modstrid med Sætning I.8.
Endelig udelukker (13) og (14) hinanden, fordi $x + z = y$ og $y + u = x$ ville føre til, at

$$(y + u) + z = y, \text{ og dermed } y + (u + z) = y,$$

atter i strid med Sætning O.8.

Sætningens slutpåstand er en direkte konsekvens af definitionen på $<$. Q.E.D.

Begrebet irrefleksiv ordningsrelation består pr. definition i irrefleksivitet, asymmetri og transitivitet. Egenskaben (18) er en tilføjelse, ikke en del af dette begreb.

Sætning I.15. Relationen $<$, indført ved definitionen ovenfor, er en irrefleksiv ordningsrelation, der opfylder: For alle $x,y,z \in \mathbb{N}$ gælder, at
(15) $x \nless x$ (irrefleksivitet)
(16) $x < y \Rightarrow y \nless x$ (asymmetri)
(17) hvis $x < y$ og $y < z$, er $x < z$ (transitivitet)
(18) enten er $x < y$, $x = y$ eller $y < x$. De tre muligheder er parvis gensidigt udelukkende. (Trichotymi)

Beviset er nærmest en reformulering af Sætning. I.14. →

En refleksiv, antisymmetrisk (læg mærke til forskellen fra asymmetrisk) og transitiv relation kaldes en refleksiv ordningsrelation. Totaliteten betyder, at vilkårlige to elementer kan sammenlignes ved relationen.

Bevis: Først bevises (15): Hvis $x < x$, fandtes pr. definition et $z \in \mathbb{N}$, så at $x + z = x$, i strid med Sætning I.8.

Til bevis for (16) antages $x < y$. Dette udsagn er i følge Sætning I.14.ensbetydende med (13). Så må $y \nless x$. Hvis nemlig $y < x$ gjaldt (Sætning I.14.) også (14), i strid med at (13) og (14) er gensidigt udelukkende hinanden.

(17) bevises således: Hvis $x < y$ og $y < z$ findes $u \in \mathbb{N}$, så at $x + u = y$,og et $v \in \mathbb{N}$, så at $y + v = z$. Men så vil $x + (u + v) = (x + u) + v = y + v = z$. Derved kan z fremstilles som sum af x og et naturligt tal (nemlig u + v), og så er $x < z$.

Endelig er (18) simpelthen en omformulering af Sætning I.14. Q.E.D.

Sammen med den irrefleksive ordningsrelation $<$, vi hidtil har arbejdet med, betragter vi den nært beslægtede refleksive ordningsrelation $\leq$. Den indføres således:

Definition: For $x,y \in \mathbb{N}$ skrives $x \leq y$ hvis og kun hvis $x < y$ eller $x = y$.

Vi skriver $x \nleq y$ for $\neg(x \leq y)$, og $x \geq y$ for $y \leq x$.

Egenskaberne ved $\leq$ fremgår af:

> Sætning I.16. For alle $x,y,z \in \mathbb{N}$ gælder, at
> (19) $x \leq x$ (refleksivitet)
> (2o) hvis $x \leq y$ og $y \leq x$ er $x = y$ (antisymmetri)
> (21)hvis $x \leq y$ og $y \leq z$ er $x \leq z$ (transitivitet)
> Hvis derudover $x < y$ eller $y < z$, vil $x < z$.
> (22) enten er $x \leq y$ eller $y \leq x$ (totalitet)

Bevis: At $\leq$ er refleksiv følger af, at for ethvert x er $x = x$ og dermed $x \leq x$. Dette beviser (19).

Antisymmetrien følger således: Lad $x \leq y$ og $y \leq x$. Vi skal vise, at $x = y$. Gjaldt dette ikke, var $x < y$ og $y < x$ i strid med asymmetrien af $<$(16). Hermed er (2o) bevist.

Bevis for (21): Lad $x \leq y$ og $y \leq z$. Hvis $x < y$ og $y < z$, er $x < z$, i følge (17). Hvis $x < y$ og $y = z$, eller hvis $x = y$ og $y < z$, er $x < z$. Hvis både $x = y$ og $y = z$, er $x = z$, og dermed $x \leq z$. Dermed er de mulige tilfælde behandlet, alle med resultatet $x \leq z$.

Endelig følger (22) umiddelbart af (18), thi hvis ikke $x = y$, må $x < y$ eller $y < x$ (p.g.a. (18). Q.E.D.

Samspillet mellem ordningen og kompositionerne + og · kommer til udtryk i

Sætning I.17. For alle $x,y,z \in \mathbb{N}$ gælder:

(23) $x < x + y$

(24) $x < y \Leftrightarrow x + z < y + z$

(25) $x \leq y \Leftrightarrow x + z \leq y + z$

(26) hvis $x \leq y$ og $u \leq v$, er $x + u \leq y + v$.
Hvis derudover $x < y$ eller $u < v$, er $x + u < y + v$
($<$ og $\leq$ harmonerer med addition)

(27) $x < y \Leftrightarrow x \cdot z < y \cdot z$

(28) $x \leq y \Leftrightarrow x \cdot z \leq y \cdot z$

(29) $x \leq x \cdot y$. Hvis $y \neq 1$, er $x < x \cdot y$

(3o) hvis $x \leq y$ og $u \leq v$ er $x \cdot u \leq y \cdot v$.
Hvis derudover $x < y$ eller $u < v$, er $x \cdot u < y \cdot v$
($<$ og $\leq$ harmonerer med multiplikation)

Bevis: Beviset består af en (lang) række simple efterprøvninger.

Ad (23): Da der findes et $z \in \mathbb{N}$ (nemlig $z = y$), så at $x + z = x + y$, er pr. definition $x < x + y$.

Ad (24):Udsagnet $x + z < y + z$ er ensbetydende med: der findes et $u \in \mathbb{N}$, så at $(x + z) + u = y + z$. På grund af forkortningsreglerne for addition er dette ensbetydende med: der fin-

des et $u \in \mathbb{N}$, så at $x + u = y$. Men det er ensbetydende med, at $x < y$.

Ad (25): Udsagnet $x + z \leq y + z$ er ensbetydende: $x + z < y + z$ eller $x + z = y + z$. I følge (24) er $x + z < y + z$ ensbetydende med $x < y$, og i følge forkortningsreglerne for addition er $x + z = y + z$ ensbetydende med $x = y$. I alt er $x + z \leq y + z$ ensbetydende med $x \leq y$.

Ad (26): Hvis $x < y$ og $u < v$ findes $z \in \mathbb{N}$, så at $x + z = y$, og $w \in \mathbb{N}$, så at $u + w = v$. Så vil

$$(x + u) + (z + w) = (x + z) + (u + w) = y + (u + w) = y + v,$$

således at $y + v$ fremgår af $x + u$ ved addition af et naturligt tal (nemlig $z + v$). Men så er $x + u < y + v$.

Hvis $x = y$ og $u < v$ har vi, at $x + u < x + v = y + v$, og hvis $x < y$ og $u = v$ gælder, at $x + u < y + u = y + v$, begge på grund af (24). Hvis endelig $x = y$ og $u = v$, er $x + u = y + v$ og dermed $x + u \leq y + v$. Dette viser (26).

Ad (27): Først antages, at $x < y$. Så findes et $u \in \mathbb{N}$, så at $x + u = y$. Dermed vil

$$x \cdot z + u \cdot z = (x + u) \cdot z = y \cdot z,$$

så at $y \cdot z$ fremgår af $x \cdot z$ ved addition af et naturligt tal (nemlig $u \cdot z$). Så er $x \cdot z < y \cdot z$.

Antages omvendt, at $x \cdot z < y \cdot z$, må $x < y$. Hvis ikke, måtte nemlig enten $x = y$ eller $y < x$ (p.g.a. (18)). Hvis $x = y$, vil $x \cdot z = y \cdot z$, i modstrid med $x \cdot z < y \cdot z$, atter p.g.a. (18). Hvis $y < x$, vil i kraft af den første halvdel: $y \cdot z < x \cdot z$, hvilket (p.g.a. (18)) ikke kan forenes med $x \cdot z < y \cdot z$.

Ad (28): Udsagnet $x \cdot z \leq y \cdot z$ er ensbetydende med: $x \cdot z < y \cdot z$ eller $x \cdot z = y \cdot z$. Her er, i følge (27), $x \cdot z < y \cdot z$

(31) siger, at ordningens forhold til efterfølgeroperationen er som man måtte vente det.

(33) fortæller, at der aldrig er plads til én til (et naturligt tal) mellem et naturligt tal og dets efterfølger. Dette er en væsentlig egenskab sammenlignet med f.eks. de rationale tals og de reelle tals egenskaber, hvor konklusionen er, at der altid mellem vilkårlige to af slagsen findes uendeligt mange flere. (Vi ser her bort fra, at vi ikke kender disse talområder endnu.)

(35) udtrykker, at S er strengt voksende.

ensbetydende med $x < y$, mens $x \cdot z = y \cdot z$ er ensbetydende med $x = y$ (p.g.a. forkortningsreglerne for multiplikation). I alt er så $x \cdot z \leq y \cdot z$ ensbetydende med $x < y$ eller $x = y$, altså med $x \leq y$.

Ad (29): Hvis $y = 1$, er $x = x \cdot 1 = x \cdot y$, og dermed $x \leq x \cdot y$. Hvis $y \neq 1$, må $y > 1$, thi p.g.a. Sætning I.2., vil y i denne situation være en efterfølger: $y = S(u) = u + 1$ for et $u \in \mathbb{N}$, således at (pr. definition) $y > 1$. Af (27) sluttes så, at $x = x \cdot 1 < y \cdot x$ ($= x \cdot y$).

Ad (3o): Hvis $x < y$ og $u < v$, findes et $z \in \mathbb{N}$, så at $x + z = y$, og et $w \in \mathbb{N}$, så at $u + w = v$. Så vil

$$y \cdot v = (x + z) \cdot (u + w) = x \cdot u + (z \cdot u + x \cdot w + z \cdot w), \text{ dvs.}$$

$y \cdot v$ fremgår af $x \cdot u$ ved addition af et naturligt tal. Så er $x \cdot u < y \cdot v$.

Hvis $x = y$ og $u < v$, har vi, at $x \cdot u < x \cdot v = y \cdot v$, og hvis $x < y$ og $u = v$ har vi, at $x \cdot u < y \cdot u = y \cdot v$, begge p.g.a. (27). Hvis endelig $x = y$ og $u = v$, er $x \cdot u = y \cdot v$ og dermed $x \cdot u \leq y \cdot v$. Dette beviser (3o) og dermed sætningen. Q.E.D.

Et par simple egenskaber samles i

Sætning I.18. For alle $x, y \in \mathbb{N}$ gælder:

(31) $S(x) > x$

(32) $x \geq 1$. Hvis $x \neq 1$, er $x > 1$.

(33) Der findes intet $z \in \mathbb{N}$, så at $x < z < S(x)$

(34) Hvis $x < y$, er $S(x) \leq y$.

(35) Hvis $x \leq y$, er $S(x) \leq S(y)$. Hvis $x < y$, er $S(x) < S(y)$.

Bevis: (31) følger af, at $S(x) = x + 1$, så at $S(x)$ fremgår af x ved addition af et naturligt tal (nemlig 1).

(32) indses således: Hvis $x = 1$, er $x \geq 1$. Hvis $x \neq 1$, er x i følge Sætning I.2. en efterfølger, dvs. $x = S(u) = u + 1$ for et $u \in \mathbb{N}$. Men så fremgår x af 1 ved addition af et naturligt tal (nemlig u). Dermed må $x > 1$.

Ad (33): Lad os antage, at der findes et $z \in \mathbb{N}$, så at $x < z < S(x)$. Så findes et $w \in \mathbb{N}$, så at $z = x + w$, og et $u \in \mathbb{N}$, så at $S(x) = z + u$. Derved må

$$x + 1 = S(x) = z + u = (x + w) + u = x + (w + u),$$

hvorved i følge forkortningsreglen for addition: $1 = w + u$. Men så vil $w < 1$ (og $u < 1$), pr. definition af $<$. Dette kan imidlertid ikke forekomme. Hvis $w = 1$, ville $1 < 1$, i strid med irrefleksiviteten af $<$. Hvis $w \neq 1$, viser (32), at $1 < w$, hvorved $w < w$, p.g.a. transitiviteten af $<$. Med det giver atter modstrid med irrefleksiviteten. Antagelsen af eksistensen af et $z \in \mathbb{N}$ med $x < z < S(x)$ giver altså konsekvenser stridende med forudgående resultater. Antagelsen må derfor være forkert.

Ad (34): Lad $x < y$. Så findes pr. definition af $<$ et $z \in \mathbb{N}$, så at $x + z = y$. Enten er nu $z = 1$, og så er $y = x + 1 = S(x)$, altså $S(x) \leq y$, eller der gælder, at $z \neq 1$. I så fald er z en efterfølger, dvs. der findes et $u \in \mathbb{N}$, for hvilket $z = S(u)$. Det giver os, at

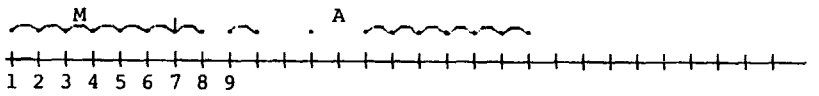
$$y = x + z = x + S(u) = S(x+u) = S(u+x) = u + S(x).$$

Det viser, at y fremgår af $S(x)$ ved addition af et naturligt tal (nemlig u), hvorved $y > S(x)$. Altså er også i dette tilfælde $y \geq S(x)$. Hermed er beviset for (34) fuldført.

Ad (35): Hvis $x < y$, findes $u \in \mathbb{N}$, så at $y = x + u$. Så vil $S(y) = S(x + u) = u + S(x)$, så at $S(y)$ fremgår af $S(x)$ ved addition af et naturligt tal (nemlig u). Men så er $S(x) < S(y)$. Hvis $x = y$ er $S(x) = S(y)$, og dermed $S(x) \leq S(y)$. Q.E.D.

Denne egenskab ved et talområde er enestående for de naturlige tal. Ikke alene har hverken de rationale tal eller de reelle tal denne egenskab. Heller ikke de hele tal har den. F.eks. har mængden A af de negative hele tal ikke noget mindste element.

Intuitivt ligger M til venstre for A på denne tallinjefigur af situationen



Det er ikke overraskende, at det må give anledning til modstrid, at man kan bevise M = $\mathbb{N}$, på grundlag af en antagelse af, at A ikke har noget mindste element.

Den følgende sætning angiver en meget væsentig egenskab ved de naturlige tal.

Sætning I.19. (De naturlige tals velordning). Mængden af de naturlige tal er velordnet. Dette betyder pr. definition, at enhver (ikke-tom) delmængde A af $\mathbb{N}$ har et mindste element, dvs. et element $m \in A$ med den egenskab, at for ethvert $x \in A$ gælder $m \leq x$.

Bevis: Lad $A \subseteq \mathbb{N}$ $(A \neq \emptyset)$ være en vilkårlig delmængde af $\mathbb{N}$. Vi beviser indirekte , at A har et mindste element. Lad os derfor antage, at dette ikke er tilfældet, og danne

$$M = \{y \in \mathbb{N} \mid \text{For ethvert } x \in A \text{ gælder: } y \leq x\}$$

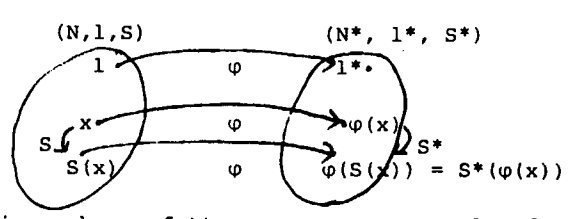
(altså mængden af elementer i $\mathbb{N}$, som er mindre end eller lig ethvert element i A).

Ved induktion vil vi godtgøre, at antagelsen om at A ikke har et mindste element, medfører at $M = \mathbb{N}$.

At $1 \in M$, dvs. at $1 \leq x$ for ethvert $x \in A$, følger af (32).

Er dernæst $y \in M$, skal det vises, at $S(y) \in M$. Det kan ikke tænkes, at $y \in A$, for så var y jo et mindste element i A, i strid med udgangsantagelsen om, at der ikke findes sådanne. Altså må $y \notin A$, og dermed, da $y \leq x$ for ethvert x i A, har vi: $y < x$ for ethvert $x \in A$. Så vil i kraft af (34): $S(y) \leq x$ for ethvert $x \in A$, hvorved $S(y) \in M$, hvilket skulle bevises. Så er altså $M = \mathbb{N}$.

Dette kan imidlertid ikke være rigtigt. For der findes ikke noget element fra A, som ligger i M, da et sådant element ville være et mindste element for A i strid med forudsætningen i det indirekte bevis.Modstriden opstod ved antagelsen om, at A ikke havde et mindste element. Denne antagelse må altså være forkert. Og sætningen er bevist. Q.E.D.



Isomorfien φ kan opfattes som en oversættelse fra N-systemet til N*-systemet, dvs. som en omdøbning af objekter og relationer, der har samme struktur, men blot omtales i forskellige sprog.

I begyndelsen af afsnittet blev det hævdet, at alle systemer som opfylder P1-P3, i en bestemt forstand er ens, således at vi uden at komme ud i problemer kan betragte hver af dem som(et eksemplar af)de naturlige tal. Vi skal nu give belæg for denne påstand. Det sker i:

Sætning I.2o. Vilkårlige to systemer (N,1,S) og (N*, 1*, S*), som opfylder P1-P3, er isomorfe, idet der findes en og kun én bijektiv afbildning (énéntydig korrespondence) $\varphi: N \sim N^*$, så at

(36) $\varphi(1) = 1^*$

(37) $\varphi(S(x)) = S^*(\varphi(x))$ for ethvert $x \in N$.

Et sådant φ vil repektere kompositionerne + og · samt ordningen <, dvs. for alle $x,y \in N$ gælder:

(38) $\varphi(x+y) = \varphi(x) +^* \varphi(y)$

(39) $\varphi(x \cdot y) = \varphi(x) \cdot^* \varphi(y)$ } (homomorfi)

(4o) $x < y \Leftrightarrow \varphi(x) <^* \varphi(y)$ (ordenstrohed)

Bevis: Beviset beror på rekursionssætningen. Den anvendes på systemet (N,1,S) med A = N*, a = 1* og g = S* . Og fortæller, at der findes en entydigt bestemt funktion $\varphi: N \sim N^*$, så at $\varphi(1) = 1^*$ og $\varphi(S(x)) = S^*(\varphi(x))$ for ethvert $x \in N$. Dette beviser, at der højst findes én funktion, der opfylder (37) og (38). For at fuldføre beviset for den første del af sætningen, skal vi indse at φ er bijektiv, dvs. injektiv og surjektiv.

At φ er surjektiv ses således: Vi sætter

$$M^* = \varphi(N) = \{x^* \in N^* \mid \exists x \in N: x^* = \varphi(x)\} .$$

Vi vil vise, ved induktion i *-systemet, at $M^* = N^*$. At $1^* \in M^*$ er oplagt, da $\varphi(1) = 1^*$. Hvis dernæst $x^* \in M^*$, dvs. $x^* = \varphi(x)$ for et $x \in N$, vil $S^*(x^*) \in M^*$. Thi $S^*(x^*) = S^*(\varphi(x)) = \varphi(S(x)) \in M^*$. Altså er $M^* = N^*$.

Vi skal nu vise, at φ er injektiv. Også dette sker ved induktion, denne gang i (N,1,S)-systemet. Vi sætter

$$M = \{x \in N \mid \text{For ethvert } y \in N \text{ gælder: } y \neq x \Rightarrow \varphi(y) \neq \varphi(x)\}$$

At $1 \in M$, dvs. for ethvert $y \in N$ gælder: $y \neq 1 \Rightarrow \varphi(y) \neq \varphi(1) = 1^*$, ses af: For $y \neq 1$, er y en efterfølger, dvs. $y = S(u)$ for et $u \in N$. Så vil $\varphi(y) = \varphi(S(u)) = S^*(\varphi(u))$. Det forhindrer, at $\varphi(y) = 1^*$. Var nemlig $\varphi(y) = 1^*$, ville $1^* \in S^*(N^*)$ i strid med P1 for *-systemet.

Antag dernæst, at $x \in M$. Det skal så vises, at $S(x) \in M$. Lad derfor $y \in N$, $y \neq S(x)$. Hvis $y = 1$, kan det ikke tænkes, at $\varphi(y) = \varphi(S(x))$, da det ville medføre, at $1^* = \varphi(1) = \varphi(y) = \varphi(S(x)) = S^*(\varphi(x))$, i strid med at $1^* \notin S^*(N^*)$. Altså er i dette tilfælde $\varphi(y) \neq \varphi(S(x))$. Hvis i stedet $y \neq 1$, er y en efterfølger, $y = S(u)$ for et $u \in N$. Var nu $\varphi(y) = \varphi(S(x))$, ville $S^*(\varphi(u)) = \varphi(S(u)) = \varphi(y) = \varphi(S(x)) = S^*(\varphi(x))$, idet de to yderste lighedstegn skyldes, at φ opfylder (37). Da S er injektiv (P2), må $\varphi(u) = \varphi(x)$. Men så må $u = x$, fordi $x \in M$, og dermed er $y = S(u) = S(x)$, i strid med forudsætningen $y \neq S(x)$. Denne modstrid opstod af antagelsen om, at $\varphi(y) = \varphi(S(x))$. Derfor må, også i dette tilfælde hvor $y \neq 1$, $\varphi(y) \neq \varphi(S(x))$. Det er derved eftervist, at for $y \in N$, $y \neq S(x)$, vil $\varphi(y) \neq \varphi(S(x))$. Dette godtgør, at $S(x) \in M$, og induktionsbeviset er fuldført.

Nu er første del af sætningen bevist.

At φ opfylder (38) indses ved induktion. Lad $x \in N$. Vi sætter

$$M_x = \{y \in N \mid \varphi(x+y) = \varphi(x) +^* \varphi(y)\}$$

Da $\varphi(x+1) = \varphi(S(x)) = S^*(\varphi(x)) = \varphi(x) +^* 1^* = \varphi(x) +^* \varphi(1)$, vil $1 \in M_x$.

Hvis $y \in M_x$, vil $S(y) \in M_x$. Thi

$$\varphi(x + S(y)) = \varphi(S(x+y)) = S^*(\varphi(x+y)) = S^*(\varphi(x)) +^* \varphi(y))$$
$$= \varphi(x) +^* S^*(\varphi(y)) = \varphi(x) +^* \varphi(S(y)),$$

hvor det første og det fjerde lighedstegn følger af (6), det andet og det sidste af (37), mens det tredje følger af induk-

tionsantagelsen $y \in M_x$. Hermed er det vist, at $M_x = N$, og (38) er bevist.

(39). Lad $x \in N$. Vi sætter

$$M_x = [y \in N \mid \varphi(x \cdot y) = \varphi(x) \cdot^* \varphi(y)] .$$

Da $\varphi(x \cdot 1) = \varphi(x) = \varphi(x) \cdot^* 1^* = \varphi(x) \cdot^* \varphi(1)$, vil $1 \in M_x$. Hvis $y \in M_x$, vil $S(y) \in M_x$. Thi

$$\varphi(x \cdot S(y)) = \varphi(x \cdot (y+1)) = \varphi(x \cdot y + x) = \varphi(x \cdot y) +^* \varphi(x)$$
$$= \varphi(x) \cdot^* (\varphi(y) +^* 1^*) = \varphi(x) \cdot^* (\varphi(y+1)) = \varphi(x) \cdot^* \varphi(S(y)),$$

hvor vi i rækkefølge har benyttet (5), (11), (38), induktionsantagelsen $y \in M_x$, (11), (38) og (5).

Endelig (4o). At $x < y$ er ensbetydende med, at der findes et $u \in N$, så at $y = x + u$. Det medfører, at $\varphi(y) = \varphi(x+u) = \varphi(x) + \varphi(u)$ (p.g.a. (38)), hvorfor $\varphi(x) <^* \varphi(y)$. Hvis omvendt $\varphi(y) >^* \varphi(x)$, må $y > x$. Thi ellers var $y \leq x$, så at enten $\varphi(y) = \varphi(x)$ eller $\varphi(x) <^* \varphi(y)$. Dermed er sætningen bevist. Q.E,D.

Om uendeligheden af mængden af naturlige tal

På intet tidspunkt i det foregående har vi i den formelle fremstilling benyttet os af et uendelighedsbegreb. Alligevel er idéen om uendeligheden af de naturlige tals mængde indstøbt i vores forestillinger om dem. Hvordan kan uendelighedsbegrebet gives en forankring i den opbygning af de naturlige tal der har fundet sted i det foregående?

Svaret er todelt. For det første er det på en række punkter opereret med en uendelighedsmekanik,uden at det er sket eksplicit. Denne mekanisme repræsenteres af efterfølgerfuntionen. Efterfølgerfunktionen vender nemlig aldrig tilbage til et punkt den har forladt. Mere præcist:

For et hvilket som helst $x \in \mathbb{N}$ gælder, at hvis $S(y) = x$, vil for $z > y$: $S(z) \neq x$. Thi af $z > y$ følger ((35), Sætning I.18), at $S(z) > S(y)$, hvorved $S(z) > x$.

Det uendelighedsbegreb der herved er tale om kunne vi kalde det ordinale uendelighedsbegreb, fordi det er knyttet til det ordningssynspunkt som ligger til grund for den måde de naturlige tal her er konstrueret på, jfr. den uformelle indledning. Man kan imidlertid - med Georg Cantor - nærme sig uendelighedsbegrebet på en lidt anden måde.

Lad os først spørge, hvad vi skal mene med at to vilkårlige, givne mængder A og B indeholder lige mange elementer. Derved mener vi, at der findes en énentydig korrespondance mellem dem. To mængder der kan bringes i énentydig korrespondance kaldes lige mægtige, eller mere latinsk, ækvipotente. Man taler også om at de har samme kardinalitet. Finessen ved denne tænkemåde er, at den hverken forudsætter en tælle- eller ordningsproces eller noget endelighedsbegreb. Den kan formuleres på mængdelæreniveau. Hvad skal vi nu i lyset heraf mene med at en mængde er endelig, respektive uendelig, hvis vi stadig ikke vil påberåbe os nogen tælleproces? Jo, siger Cantor, dermed skal vi mene, at mængden ikke kan bringes i énentydig korrespondance med nogen ægte delmængde af den selv. Ved en uendelig mængde må vi så selvfølgelig forstå en mængde, der ikke er endelig, altså én der kan bringes i énentydig korrepondance med en eller anden ægte delmængde med den selv. Det leder os til

Definition. En mængde A kaldes endelig, hvis der ikke findes nogen ægte (ikke-tom) delmængde af A, som står i énentydig korrespondance med A. En mængde A kaldes uendelig, hvis der findes en ægte (ikke-tom) delmængde af A og en bijektiv afbildning $f: A \sim A$.

Vi kunne kalde det uendelighedsbegreb der fastlægges her, det kardinale uendelighedsbegreb.

Det er nu en gratis sag at indse, at de naturlige tal også i

denne forstand er en uendelig mængde. At dette hænger nøje sammen med den ordinale uendelighed - gennem efterfølgerfunktionen - skulle ikke overraske.

Sætning. I.21. De naturlige tals mængde er (kardinalt) uendelig, dvs. der findes en ægte, ikke-tom delmængde A af $\mathbb{N}$, og en bijektiv afbildning $f: \mathbb{N} \sim A$.

Bevis. Vi sætter $A = S(\mathbb{N})$ og $f = S$. Så er $S(\mathbb{N})$ en ægte delmængde af $\mathbb{N}$ (i følge P1 gælder $1 \notin S(\mathbb{N})$), og f er en injektiv afbildning. Den er selvsagt surjektiv på sin værdimængde $f(\mathbb{N}) = S(\mathbb{N})$.

Herefter er der ikke noget i vejen for at anvende mængden af naturlige tal som prototype for en bestemt slags uendelige mængder. Vi vedtager:

Definition. En mængde A kaldes tællelig, eller numerabel, hvis den er ækvipotent med $\mathbb{N}$.

Det er oplagt at enhver tællelig mængde er (kardinalt) uendelig.

*

Vi burde slutte behandlingen af de naturlige tal med at godtgøre at ethvert naturligt tal, forskelligt fra 1, kan tjene som grundtal for en positionsfremstilling af de naturlige tal. Dette kan imidlertid ikke formuleres tilstrækkelig fornuftigt (men kan dog formuleres), før de naturlige tal er blevet suppleret med tallet o, hvilket sker i det næste kapitel.

II. DE HELE TAL.

Udvidelsen af de naturlige tal til de hele tal

Uformel indledning

Den idé der ligger bag udvidelsen af de naturlige tal til de hele tal, kan belyses ved betragtning af subtraktionen m-n for m,n ∈ ℕ. Hvis m > n giver denne subtraktion mening inden for ℕ, og resulterer i et naturligt tal, mens det ikke er muligt inden for de naturlige tals mængde at udføre subtraktionen hvis m ≤ n. Den umiddelbare idé er så at supplere de naturlige tal med sådanne objekter, der kan siges at fremgå af en "utilladelig" subtraktion. Hvordan kan dette gøres?

En tilladelig subtraktion kan opfattes som sendende visse par (nemlig dem hvis første-komponent er større end anden-komponenten) (m,n) af naturlige tal over i naturlige tal, nemlig m-n. Hvis man i én eller anden forstand identificerer m-n (hvor m > n) med parret (m,n), kan man lige så vel lade m-n, hvor m ≤ n, betyde pr. definition parret (m,n), der jo er veldefineret.

Altså første idé: for m,n ∈ ℕ "identificeres" m-n med (m,n). Her melder sig den første vanskelighed. Eftersom et naturligt tal p på uendelig mange måder kan fremstilles som differens mellem to naturlige tal, kan man ikke uden videre pege på det par (m,n) af naturlige tal, der skal repræsentere p. Dette problem må løses, før vi drømmer om at gennemføre identifikationen også til par (m,n), hvor m ≤ n.

Anden idé: vi lader alle par, hvis differens er et givet tal, være ækvivalente. Med andre ord: vi søger at indføre en ækvivalensrelation i ℕxℕ. Imidlertid kan vi jo ikke så godt definere, at to par er ækvivalente hvis og kun hvis de har samme differens mellem første og anden komponent, så længe denne differens ikke har mening for ethvert par. Vi må derfor foretage en omformulering af den angivne ækvivalens"definition". Dette sker ved at vi observerer, at m-n = m_1-n_1 er ensbetydende med, at m+n_1 = m_1+n, hvilket har mening for alle m,n,m_1,n_1 i ℕ.

Når vi udvider subtraktionen af naturlige tal til situationer, hvor den ikke i forvejen har mening, må vi sikre at det udvidede område kommer til at besidde acceptable egenskaber, hvortil f.eks. hører at subtraktion af to af de nye objekter altid kan udføres. Vi ønsker jo ikke at blive stillet over for et behov for nye udvidelser til at klare subtraktionsproblemerne. Det anførte krav kommer ud på, at de udvidede objekter ved den addition vi skal introducere blandt dem, skal udgøre en gruppe.

Vi kan nu opsummere vores udvidelsesønsker således:

Vi søger en mængde ℤ og en komposition + i ℤ, så at

(1) (ℤ,+) er en gruppe,

(2) (ℕ,+) i én eller anden forstand kan opfattes som en delmængde af (ℤ,+),

(3) ethvert element i ℤ kan fremstilles som differens (jfr. (2)) af to elementer fra ℕ.

Proceduren i det følgende vil være at realisere dette ønske gennem en sætning, der gælder i den konkrete situation. Men sætningen er i virkeligheden et specialtilfælde af en generel sætning fra algebraen. Når sætningen ikke er formuleret i sin generelle form, hvad der ikke ville have været teknisk vanskeligere, fordi beviset er praktisk taget identisk med det der gives, skyldes det et ønske om at forankre det der foregår i forståelsen af den konkrete situation, samt et ønske om ikke på dette sted at involvere mere abstrakt algebra end nødvendigt.

*

I forhold til de naturlige tal leverer de hele tal en udvidelse med tallet nul og med de negative hele tal. Fra et strukturelt synspunkt, hvor man hæfter sig ved graden af algebraisk kompleksitet, befinder de hele tal sig på det næst-første stadium i talsystemhierarkiet. Historisk set forholder det sig anderledes. Længe før både tallet nul og de negative hele tal blev taget i betragtning i matematikken havde man arbejdet med (positive) brøker, altså rationale tal. Det var f.eks. både

tilfældet i mesopotamisk matematik (fra 3ooo f.v.t.) og i ægyptisk matematik (fra 18oo f.v.t.).

Inddragelsen af nullet og de negative tal tog lang tid og forløb i flere faser. Mesopotamerne noterede meget tidligt de naturlige tal i et positionssystem, med grundtallet 6o. Det forudsætter, at det er muligt i opskrivningen at markere at visse 6o-potenser kan mangle, som i tallet $17\cdot 60^2+11\cdot 60^0$, hvor potensen 60^1 ikke indgår. I begyndelsen levede mesopotamerne med de flertydigheder der kommer heraf, ligesom de levede med andre flertydigheder i talnotationen, f.eks. foranlediget af manglen på en absolut plads, "pladsen før kommaet". Man måtte af sammenhængen slutte hvad der var tale om. Lidt senere efterlod man en tom plads, hvis den dertil svarende 6o-potens ikke bidrog med noget led, og endnu senere indførtes et særligt tegn til at anbringe på (tal)tomme pladser. Dette skridt repræsenterer første fase af nullets fødsel: erkendelsen af at "ingenting" kræver en benævnelse og et særligt tegn. Der blev imidlertid aldrig tale om at mesopotamerne regnede med nul som et tal. Det skridt blev først taget fuldt ud i det 9. årh. e.v.t. af inderne, og antagelig senest samtidig af kineserne. I senest det 5. årh.benyttedes i indisk matematik ordet *sunya* (det tomme) for nul som et tal. På arabisk blev det til *al-cifr*, og derfra på europæisk til "ciffer", som altså betød nul, indtil Gauss. Selve tegnet o for nul findes hos inderne i det 7. århundrede e.v.t. Regning med nul som et tal på linje med andre kendes først hos inderen Sridhara (o. 85o-95o e.v.t.), der har nedskrevet regnereglerne a±o = a, o+a = a, a-a = o, a·o = o·a = o, o:a = o. Processen fra fortolkning af et nulbegreb, over indførelsen af et nultegn, videre over begrebet om nul som et tal med en eller anden form for eksistens, frem til nul som et tal der kan regnes med, dvs. som kan indgå i algebraiske operationer, tog altså henved to tusinde år.

Nogenlunde lige sådan forholdt det sig med de negative hele tal, blot parallelforskudt nogle hundrede år i retning af vor tid. I babyloniske astronomiske tabeller fra o. 6oo f.v.t. har man fundet negative tal, men som referende til noget bestemt i den givne astronomiske sammenhæng, ikke til selvstændige tal.

Inderne opererede tidligt med muligheden af i bestemte (økonomiagtige) forbindelser at fortolke hvad der svarer til negative tal. Man brugte om de positive tal ordet *dhana* (ejendom) og om de negative *kšaya* (skyld). Tegn for negative tal kendes hos Brahmagupta (o. 6oo f.v.t.) og i kinesisk matematik (o. 2oo f.v.t.). Der var her også tale om operationer med dem, men kun knyttet til mellemregninger. De blev ikke anset som acceptable slutresultater af problemløsninger, og stadig ikke som tal med egen eksistens(berettigelse).

Leonardo af Pisa (Fibonacci) anerkendte o. 12oo e.v.t. som den første negative tal som svar på opgaver, men i forbindelser hvor negativiteten kunne tilskrives en rimelig virkelighedsfortolkning. Skridtet til at anskue de negative tal abstrakt, frigjort fra fortolkningsbindinger, og til at underkaste dem aritmetiske operationer, blev først taget af Chuquet (1484). Helt op i 16oo-tallet talte man om de negative tal som fiktive, og om falske løsninger når de forekom.

Den fremstilling vi i det følgende skal give af de hele tal, skriver sig fra slutningen af det 19. årh. og indgik i de almindelige bestræbelser på at konstruere talsystemet. Modellen til den konstruktion vi skal udføre i det følgende stammer fra H. Weber (1895), hvor den havde en lidt anden skikkelse. Det algebraiske begrebsapparat (integritetsring m.m.) vi skal tage i anvendelse udmøntedes af Kronecker og Dedekind i årtierne før.

Den generelle sætning, som den foreliggende er et specialtilfælde af, går ud på, at enhver kommutativ semigrupppe hvori forkortningsreglerne gælder, på entydig måde kan udvides til en gruppe, hvor udvidelse skal forstås i betydningen (1) og (2). Beviset for den speciellere Sætning II.1. benytter om $(\mathbb{N},+)$ kun at den er en kommutativ semigrupppe hvori forkortningsreglerne gælder. Beviset kan derfor opfattes som gældende også for den generelle sætning.

Når sætningen er bevist vil vi i stedet for G bruge betegnelsen $\mathbb{Z}$, og i stedet for $\tilde{+}$ blot +.

For en oversigt over de første bevisidéer henvises til den uformelle indledning.

At $\oplus$ må defineres således bliver klart, når vi tænker på at (m_1,n_1) står for m_1-n_1 og (m_2,n_2) for m_2-n_2, og dermed summen af parrene for $(m_1-n_1)+(m_2-n_2) = (m_1+m_2)-(n_1+n_2)$, der repræsenteres af parret (m_1+m_2,n_1+n_2).

Check selv associativiteten og kommutativiteten af $\oplus$. Læg mærke til at der kun benyttes, at + i $\mathbb{N}$ er associativ og kommutativ.

Beviset for at $\sim$ er transitiv anvender - ud over at + er associativ og kommutativ - at forkortningsreglerne gælder i $(\mathbb{N},+)$.

Udvidelsen af de naturlige tal til de hele tal

Vi fanger straks an med at formulere og bevise den sætning som blev omtalt i den uformelle indledning.

Sætning II.1. Der findes en kommutativ gruppe $(G,\tilde{+})$ som har følgende egenskaber:

(1) Der findes en delmængde $(\tilde{\mathbb{N}},\tilde{+})$ af $(G,\tilde{+})$ der er isomorf med $(\mathbb{N},+)$.

(2) Ethvert element g i G kan skrives på formen
$g = \tilde{m} \tilde{-} \tilde{n}$
for et $\tilde{m}$ og et $\tilde{n}$ i $\tilde{\mathbb{N}}$. (Her betegner $\tilde{m} \tilde{-} \tilde{n}$ elementet $\tilde{m} \tilde{+} (\tilde{n})^{-1}$ i G.)

Gruppen $(G,\tilde{+})$ er entydigt bestemt pånær isomorfi, således at forstå, at hvis $(G',\tilde{+}')$ er en kommutativ gruppe der opfylder (1) og (2) (med de oplagte notationsmæssige korrektioner), findes en isomorfi fra $(G,\tilde{+})$ til $(G',\tilde{+}')$ ved hvilken $(\mathbb{N},+)$ er isomorf med $(\tilde{\mathbb{N}}',\tilde{+}')$.

Bevis. Beviset falder i to hoveddele, hvor første del drejer sig om eksistensen af $(G,\tilde{+})$, og anden del drejer sig om entydigheden.

Eksistensen:

Vi lægger ud med at definere kompositionen $\oplus$ i $\mathbb{N}\times\mathbb{N}$ ved for vilkårlige (m_1,n_1) og (m_2,n_2) i $\mathbb{N}\times\mathbb{N}$ at sætte

(3) $(m_1,n_1) \oplus (m_2,n_2) = (m_1+m_2,n_1+n_2)$.

Denne komposition er åbenbart associativ og kommutativ, fordi + er det.

Dernæst defineres i $\mathbb{N}\times\mathbb{N}$ relationen $\sim$

(4) $\forall (m_1,n_1), (m_2,n_2) \in \mathbb{N}\times\mathbb{N}: (m_1,n_1) \sim (m_2,n_2) \Leftrightarrow m_1+n_2 = m_2+n_1$

Denne relation er tydeligvis refleksiv og symmetrisk. Den er også transitiv, altså i alt en ækvivalensrelation.

Transitiviteten ses således: Af
$(m_1,n_1) \sim (m_2,n_2)$ og $(m_2,n_2) \sim (m_3,n_3)$
sluttes, at

Endnu engang beror argumenterne kun på associativiteten og kommutativiteten af +.

$m_1+n_2 = m_2+n_1$ og $m_2+n_3 = m_3+n_2$,
der ved addition af venstre- og højresider giver
$(m_1+n_2)+(m_2+n_3) = (m_2+n_1)+(m_3+n_2)$.
Anvendes her kommutativiteten og associativiteten af +, kan denne identitet omformes til
$m_1+n_3+(n_2+m_2) = m_3+n_1+(n_2+m_2)$.
Men fordi forkortningsreglerne gælder i $(\mathbb{N},+)$, følger
$m_1+n_3 = m_3+n_1$,
hvilket netop er betingelsen for at
$(m_1,n_1) \sim (m_3,n_3)$.

Den betragtede ækvivalensrelation harmonerer med $\oplus$.

Lad nemlig $(m_1,n_1) \sim (m_2,n_2)$ og $(p_1,q_1) \sim (p_2,q_2)$.
Vi skal vise, at
$(m_1,n_1) \oplus (p_1,q_1) \sim (m_2,n_2) \oplus (p_2,q_2)$,
hvilket i kraft af (3) kommer ud på at vise, at
$(m_1+p_1,n_1+q_1) \sim (m_2+p_2,n_2+q_2)$,
hvilket på sin side pr. definition af $\sim$ kommer ud på at vise, at
$(m_1+p_1)+(n_2+q_2) = (n_1+q_1)+(m_2+p_2)$.
Men da nu på grund af forudsætningerne
$m_1+n_2 = m_2+n_1$ og $p_1+q_2 = p_2+q_1$,
fremgår den ønskede identitet af disse to ved addition og ommøblering under anvendelse af associativiteten og kommutativiteten af +.

Opsamling: Ved (3) er der defineret en komposition $\oplus$ i $\mathbb{N}\times\mathbb{N}$, der er associativ og kommutativ. Ved (4) er der defineret en ækvivalensrelation $\sim$, der harmonerer med $\oplus$.

Lad os nu betragte mængden af ækvivalensklasser i $\mathbb{N}\times\mathbb{N}$ modulo $\sim$. Denne mængde betegnes G. Klasserne i kvotientmængden betegnes med Γ-er. Den klasse der indeholder (m,n) som repræsentant betegnes med $\Gamma_{(m,n)}$. Vi ønsker at definere en komposition $\tilde{+}$ i G, altså på ækvivalensklasserne. Til dette formål udnyttes den af $\oplus$ inducerede komposition på kvotientmængden (jfr. "Algebraiske forberedelser"). Betegnes den med $\tilde{+}$, er den defineret ved

(5) $\forall \Gamma_1,\Gamma_2 \in G: \Gamma_1 \tilde{+} \Gamma_2 = \Gamma_{(m_1,n_1)} \tilde{+} \Gamma_{(m_2,n_2)} \stackrel{D}{=} \Gamma_{(m_1+m_2,n_1+n_2)}$,

hvor (m_1,n_1) og (m_2,n_2) er vilkårlige repræsentanter i hen-

Intuitivt skal vi tænke på de neutrale element som "o". Imidlertid eksisterer o jo ikke i $\mathbb{N}$. Men da vi forestiller os de hele tal som differenser m-n af naturlige tal, skal vi tænke på "o" som klassen af differenser af formen m-m.

I daglig omgang med de hele tal er den inverse ved addition til m-n lig med n-m. Det er derfor ikke overraskende, at den inverse til klassen $\Gamma_{(m,n)}$ er $\Gamma_{(n,m)}$.

Hvis vi minder om den uformmele indledning skal vi nå til at betragte alle "differenser" m-n for m,n i $\mathbb{N}$. Hvis vi blandt disse skulle udpege de naturlige tal, ville det jo være fristende at pege på differenserne af formen m-o, men det kan jo altså ikke lade sig gøre, da o $\notin \mathbb{N}$. I stedet må vi hæfte os ved differenser af formen (m+p)-p for m,p i $\mathbb{N}$. Dette leder frem til klassen $\Gamma_{(m+p,p)}$ der viser sig kun at afhænge af m, ikke af p.

holdsvis Γ_1 og Γ_2. Fra den almindelige teori vides, at dette giver mening uanset valget af repræsentanter, og at $\tilde{+}$ er kommutativ fordi $\oplus$ er det.

Hvis nu m er et vilkårligt element i $\mathbb{N}$ består $\Gamma_{(m,m)}$ af alle par af formen (n,n), n $\in \mathbb{N}$.

Thi af (u,v) $\in \Gamma_{(m,m)}$ er ensbetydende med at u+m = v+m, der er ensbetydende med at u = v, på grund af forkortningsreglen for addition i $\mathbb{N}$.

Betegner nu E klassen $\Gamma_{(m,m)}$, ses at for ethvert $\Gamma \in G$ gælder, (idet (p,q) er en vilkårlig repræsentant i Γ), at

$$E \tilde{+} \Gamma_{(p,q)} = \Gamma_{(m+p,m+q)} = \Gamma_{(p,q)}.$$

Det sidste lighedstegn følger af, at (r,s) $\in \Gamma_{(m+p,m+q)}$ hvis og kun hvis

r+(m+q) = s+(m+p),

hvilket er ensbetydende med, at

(r+q)+m = (s+p)+m.

Denne sidste identitet er ækvivalent (forkortningsreglerne gælder i $(\mathbb{N},+)$) med, at r+q = s+p, der netop er betingelsen for, ar (r,s) $\in \Gamma_{(p,q)}$.

Den viste sammenhæng udtrykker, at E er neutralt element ved $\tilde{+}$ i G.

For at have vist at $(G,\tilde{+})$ er en kommutativ gruppe, mangler vi at indse, at ethvert element har et inverst. Lad derfor Γ være et vilkårligt element i G, og lad (m,n) være en vilkårlig repræsentant for Γ. Så vil altså $\Gamma = \Gamma_{(m,n)}$. Nu påstås, at $\Gamma_{(n,m)}$ er inverst til $\Gamma_{(m,n)}$. Der gælder jo

$$\Gamma_{(m,n)} \tilde{+} \Gamma_{(n,m)} = \Gamma_{(m+n,n+m)} = E.$$

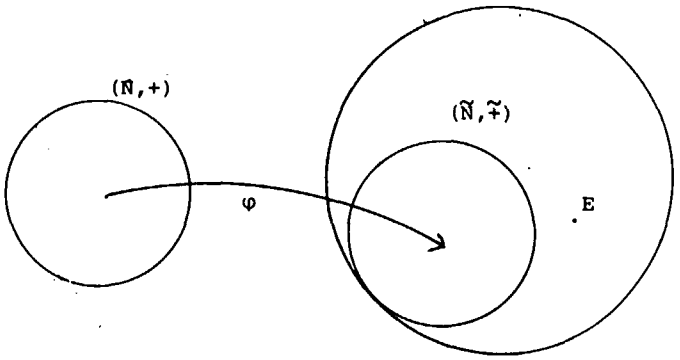
Hermed er $(G,\tilde{+})$ en kommutativ gruppe.

Den næste opgive bliver at bevise (1), altså at der findes en delmængde $(\tilde{\mathbb{N}},\tilde{+})$ af $(G,\tilde{+})$ der er isomorf med $(\mathbb{N},+)$. Vi betragter for ethvert m $\in \mathbb{N}$ ækvivalensklassen

$$\Gamma^m = \Gamma_{(m+p,p)}$$

hvor p er et vilkårligt naturligt tal.

$(G,\tilde{+}) = (\mathbb{N}x\mathbb{N}/\sim,\tilde{+})$



Det neutrale element $E = \Gamma_{(m,m)}$ ligger ikke i $\tilde{\mathbb{N}}$. Thi var det tilfældet ville

$$\Gamma_{(m,m)} = \Gamma_{(n+p,p)} \text{ for et } n,p \in \mathbb{N},$$

hvilket ville afstedkomme m+p=m+n+p, og dermed m = m+n (forkortningsreglen i ℕ), i strid med Sætning I.8.

Det ses, at $\Gamma_{(m+p,p)} = \{(m+q,q) \mid q \in \mathbb{N}\}$, idet $(r,s) \in \Gamma_{(m+p,p)}$ præcis hvis r+p = (m+p)+s, dvs. netop hvis (forkortningsreglen i ℕ) r = m+s, altså netop hvis (r,s) = (m+s,s).

Derved er $\Gamma^m = \{(m+q,q) \mid q \in \mathbb{N}\}$.

Defineres nu afbildningen

$$\varphi: \mathbb{N} \sim \tilde{\mathbb{N}}$$

ved

$$\varphi(m) = \Gamma^m, \; m \in \mathbb{N},$$

er φ bijektiv. Lad nemlig Γ^m være et vilkårligt element i $\tilde{\mathbb{N}}$. Da Γ^m er billedet af m ved φ, er φ surjektiv. Er endvidere

$$\varphi(m_1) = \varphi(m_2), \text{ dvs. } \Gamma^{m_1} = \Gamma^{m_2},$$

er $m_1 = m_2$, dvs. φ er injektiv.

Dette indses således: For et vilkårligt $p \in \mathbb{N}$ vil

$$(m_1+p,p) \in \Gamma^{m_1} = \Gamma^{m_2} = \{(m_2+q,q) \mid q \in \mathbb{N}\},$$

hvorfor der findes et $q \in \mathbb{N}$, så at

$$(m_1+p,p) = (m_2+q,q).$$

Her må q = p og dermed $m_1+p = m_2+p$, hvoraf vi slutter (fordi forkortningsreglerne gælder i (ℕ,+)), at $m_1 = m_2$.

Kan vi ydermere vise, at φ er en homomorfi, er <u>φ en isomorfi</u> mellem (ℕ,+) og $(\tilde{\mathbb{N}},\tilde{+})$, og (1) er bevist. Og det kan vi.

Vi har $\varphi(m_1+m_2) = \Gamma^{m_1+m_2} = \{(m_1+m_2+q,q) \mid q \in \mathbb{N}\}$ og $\Gamma^{m_1} \tilde{+} \Gamma^{m_2} = \Gamma_{(m_1+r,r)} \tilde{+} \Gamma_{(m_2+s,s)} = \Gamma_{(m_1+m_2+r+s,r+s)}$, hvor (m_1+r,r) er en vilkårlig repræsentant for klassen Γ^{m_1}, og (m_2+s,s) er en vilkårlig repræsentant for Γ^{m_2}. Da desuden $(m_1+m_2+r+s,r+s)$ er en repræsentant for $\Gamma^{m_1+m_2}$, ses at $\varphi(m_1)+\varphi(m_2) = \Gamma^{m_1} \tilde{+} \Gamma^{m_2} = \Gamma^{m_1+m_2} = \varphi(m_1+m_2)$, hvilket beviser, at φ er en homomorfi.

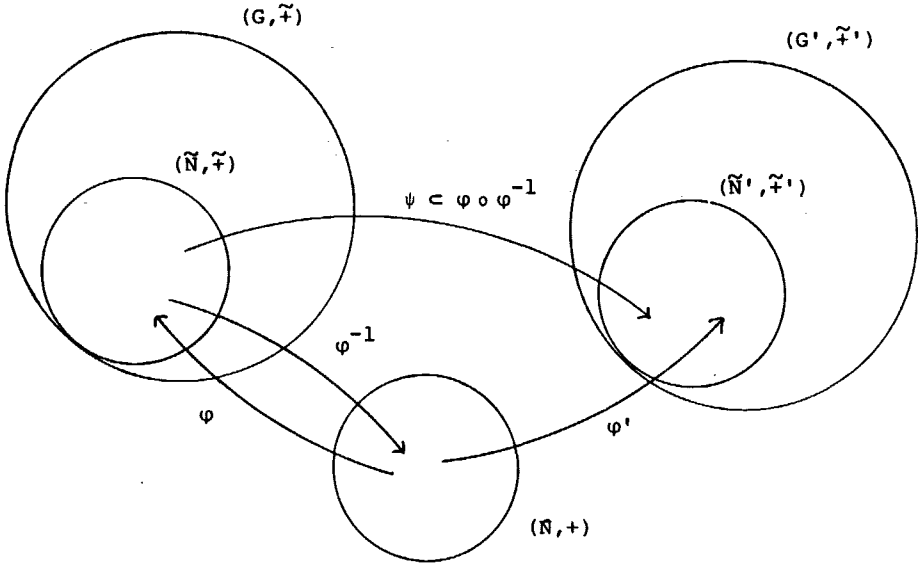
<u>Hermed er (1) bevist</u>. Vi bruger nu betegnelsen $\tilde{m}$ om $\varphi(m) = \Gamma^m$.

Vi skal dernæst vise (2): ethvert element g i G kan skrives på formen

$$g = \tilde{m} \tilde{-} \tilde{n} = \tilde{m} \tilde{+} (\tilde{n})^{-1}$$

for et $\tilde{m},\tilde{n}$ i $\tilde{\mathbb{N}}$.

Læg i øvrigt endnu engang mærke til, at beviset beror på forkortningsreglerne i $(\mathbb{N},+)$



Den lidt teknisk betonede gymnastik i dette afsnit skyldes, at vi for at kunne hævde at (6) er en definition, må være sikre på, at vi ikke ville have fået en anden fastlæggelse af φ, hvis vi tilfældigvis havde valgt en anden fremstilling af g.

Det er en pointe, at beviset for hele entydighedsdelen kun beror på egenskaberne ved $(\tilde{\mathbb{N}},\tilde{+})$ og $(\tilde{\mathbb{N}}',\tilde{+}')$ og ikke på $(\mathbb{N},+)$'s egenskaber direkte.

Da g har formen $g = \Gamma_{(m,n)}$ for et par (m,n) i $\mathbb{N}\times\mathbb{N}$, og da

$$\Gamma_{(m,n)} = \Gamma_{(m+p+q,n+p+q)} = \Gamma_{(m+p,p)} \tilde{+} \Gamma_{(q,q+n)} =$$
$$\Gamma_{(m+p,p)} \tilde{+} \Gamma_{(n+q,q)}^{-1} = \Gamma^m \tilde{+} (\Gamma^n)^{-1} = \tilde{m} \tilde{-} \tilde{n},$$

for et $\tilde{m}$ og et $\tilde{n}$ i $\tilde{\mathbb{N}}$, har g den ønskede form.

Hermed er (2) bevist. Det betyder, at beviset for eksistensen af $(G,\tilde{+})$ er nu gennemført. Tilbage står

Entydigheden:

Antager vi, at $(G',\tilde{+}')$ har de samme egenskaber som $(G,\tilde{+})$ (med de relevante notationsændringer), skal vi indse, at der findes en isomorfi $\psi: G \sim G'$, og at også $(\tilde{\mathbb{N}},\tilde{+})$ og $(\tilde{\mathbb{N}}',\tilde{+}')$ er isomorfe ved denne isomorfi.

Den søgte isomorfi tilvejebringes ved at der først etableres en isomorfi mellem $\tilde{\mathbb{N}}$ og $\tilde{\mathbb{N}}'$ og derefter foretages en udvidelse af denne isomorfi til $\tilde{G}$ på $\tilde{G}'$.

Der findes (i kraft af beviset for eksistensen) en isomorfi $\varphi: \mathbb{N} \sim \tilde{\mathbb{N}}$ og (efter antagelsen i dette afsnit) en isomorfi $\varphi': \mathbb{N} \sim \tilde{\mathbb{N}}'$. Ved

$$\psi' = \varphi' \circ \varphi^{-1}: \tilde{\mathbb{N}} \sim \tilde{\mathbb{N}}'$$

defineres en isomorfi fra $\tilde{\mathbb{N}}$ til $\tilde{\mathbb{N}}'$. For at vise, at ψ' kan udvides til en isomorfi ψ fra G til G', benytter vi, at ethvert g i G kan skrives på formen $g = \tilde{m} \tilde{-} \tilde{n}$ for et $\tilde{m}$ og et $\tilde{n}$ i $\tilde{\mathbb{N}}$. Sættes

$$(6) \quad \psi(g) = \psi'(\tilde{m}) \tilde{-}' \psi'(\tilde{n}) \quad (= \psi'(\tilde{m}) \tilde{+}' (\psi'(\tilde{n}))^{-1})$$

fås en tilladelig definition.

Vi skal for at kunne hævde dette indse, at hvis $g = \tilde{m}_1 \tilde{-} \tilde{n}_1$ for et $\tilde{m}_1$ og et $\tilde{n}_1$ er en anden fremstilling af g, vil

$$\psi'(\tilde{m}) \tilde{-}' \psi'(\tilde{n}) = \psi'(\tilde{m}_1) \tilde{-}' \psi'(\tilde{n}_1),$$

hvilket er ensbetydende med, at

$$\psi'(\tilde{m}) \tilde{+}' (\psi'(\tilde{n}))^{-1} = \psi'(\tilde{m}_1) \tilde{+}' (\psi'(\tilde{n}_1))^{-1}.$$

Men dette er, da $\tilde{+}'$ er kommutativ, på sin side ensbetydende med, at

$$\psi'(\tilde{m}) \tilde{+}' \psi'(\tilde{n}_1) = \psi'(\tilde{m}_1) \tilde{+}' \psi'(\tilde{n}).$$

Udnytter vi, at ψ' er en homomorfi fra $(\tilde{\mathbb{N}},\tilde{+})$ til $(\tilde{\mathbb{N}}',\tilde{+}')$

ser vi, at vi alt i alt skal godtgøre, at
$\psi'(\tilde{m} \tilde{+} \tilde{n}_1) = \psi'(\tilde{m}_1 \tilde{+} \tilde{n})$.
Men da $g = \tilde{m} \tilde{-} \tilde{n} = \tilde{m}_1 \tilde{-} \tilde{n}_1$, og dermed
$\tilde{m} \tilde{+} \tilde{n}_1 = \tilde{m}_1 \tilde{+} \tilde{n}$,
følger, at
$\psi'(\tilde{m} \tilde{+} \tilde{n}_1) = \psi'(\tilde{m}_1 \tilde{+} \tilde{n})$.

Efter således at have indset, at der ved (6) defineres en afbildning ψ fra G til G', mangler vi at indse, at ψ er en isomorfi.

At ψ er en homomorfi indses således:

Lad g_1 og g_2 være vilkårlige elementer i G. Så findes $\tilde{m}_1, \tilde{n}_1$ og $\tilde{m}_2$, $\tilde{n}_2$ i $\tilde{N}$, så at
$g_1 = \tilde{m}_1 \tilde{-} \tilde{n}_1$ og $g_2 = \tilde{m}_2 \tilde{-} \tilde{n}_2$.
Derved bliver
$g_1 \tilde{+} g_2 = (\tilde{m}_1 \tilde{+} \tilde{m}_2) \tilde{-}' (\tilde{n}_1 \tilde{+} \tilde{n}_2)$
og dermed
$\psi(\tilde{g}_1 \tilde{+} \tilde{g}_2) = \psi'(\tilde{m}_1 \tilde{+} \tilde{m}_2) \tilde{-}' \psi'(\tilde{n}_1 \tilde{+} \tilde{n}_2)$
$= (\psi'(\tilde{m}_1) \tilde{-}' \psi'(\tilde{n}_1)) \tilde{+}' (\psi'(\tilde{m}_2) \tilde{-} \psi'(\tilde{n}_2))$
$= \psi(g_1) \tilde{+}' \psi(g_2)$,
der netop er betingelsen for, at ψ er en homomorfi.

At ψ er injektiv fremgår af,
at man (for $g_1 = \tilde{m}_1 \tilde{-} \tilde{n}_1$ og $g_2 = \tilde{m}_2 \tilde{-} \tilde{n}_2$) af
$\psi(g_1) = \psi(g_2)$
kan slutte, at
$\psi'(\tilde{m}_1) \tilde{-}' \psi'(\tilde{n}_1) = \psi'(\tilde{m}_2) \tilde{-}' \psi'(\tilde{n}_2)$,
og dermed at
$\psi'(\tilde{m}_1 \tilde{+} \tilde{n}_2) = \psi'(\tilde{m}_2 \tilde{+} \tilde{n}_1)$.
Eftersom ψ' er injektiv vil
$\tilde{m}_1 \tilde{+} \tilde{n}_2 = \tilde{m}_2 \tilde{+} \tilde{n}_1$,
og dermed
$\tilde{m}_1 \tilde{-} \tilde{n}_1 = \tilde{m}_2 \tilde{-} \tilde{n}_2$,
hvilket netop udtrykker, at $g_1 = g_2$.

For at indse at ψ er surjektiv, betragter vi et vilkårligt element g' i G', og skal finde et g i G, for hvilket $\psi(g) = g'$.

Det sker således: Der findes $\tilde{m}'$ og $\tilde{n}'$ i $\tilde{N}'$, så at
$g' = \tilde{m}' \tilde{-} \tilde{n}'$. Da ψ' er surjektiv findes $\tilde{m}$ og $\tilde{n}$ i $\tilde{N}$, så at
$\psi'(\tilde{m}) = \tilde{m}'$ og $\psi'(\tilde{n}) = \tilde{n}'$. Men så er med $g = \tilde{m} \tilde{-} \tilde{n}$ ($\in G$)

Det er vigtigt at forstå denne identifikation som knyttet til eksistensen af isomorfien og ikke som et skift i definitionen af mængden af naturlige tal. Identifikationen kan udtrykkes: I henseende til algebraiske egenskaber er $(\mathbb{N},+)$ og $(\tilde{\mathbb{N}},\tilde{+})$ ens.

$g' = \psi'(\tilde{m}) \tilde{=} \psi'(\tilde{n}) = \psi(g)$,
hvilket viser surjektiviteten.

Til sidst skal vi godtgøre at ψ er en udvidelse af ψ'.

Men det kommer af, at for $\tilde{m} \in \tilde{\mathbb{N}}$ er
$\tilde{m} = (\tilde{m} \tilde{+} \tilde{m}) \tilde{-} \tilde{m}$,
hvorved
$\psi(\tilde{m}) = \psi'(\tilde{m} \tilde{+} \tilde{m}) \tilde{-}' \psi'(\tilde{m}) = \psi'(\tilde{m}) \tilde{+}' \psi'(\tilde{m}) \tilde{-}' \psi'(\tilde{m})$
$= \psi'(\tilde{m})$.
(Heraf følger, at ikke kun ved ψ' er $(\tilde{\mathbb{N}},\tilde{+})$ isomorf med $(\tilde{\mathbb{N}}',\tilde{+}')$, men også ved ψ.)

Hermed er beviset for Sætning II.1 fuldført.

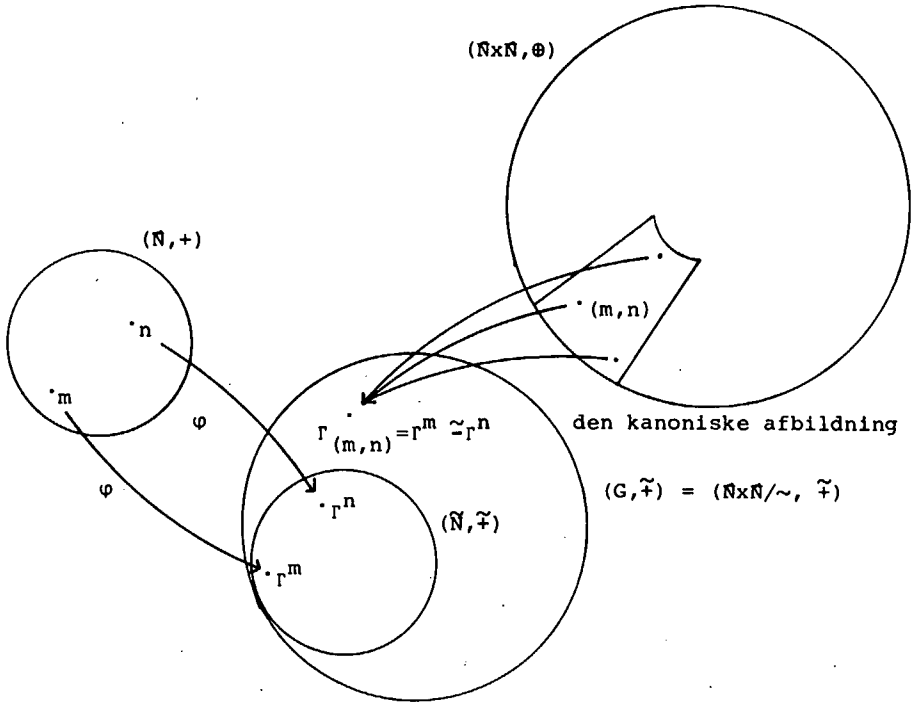
Elementerne i G kaldes de hele tal. I stedet for G skrives normalt $\mathbb{Z}$. Eftersom konstruktionen er udført for at udvide mængden af naturlige tal til mængden af hele tal, er det rimeligt at identificere semigruppen $(\mathbb{N},+)$ med den dermed isomorfe delmængde $(\tilde{\mathbb{N}},\tilde{+})$ af $(G,\tilde{+})$. Vi taler om at $(\mathbb{N},+)$ er indlejret i $(G,\tilde{+})$, eller i $(\mathbb{Z},+)$. Dette giver ikke anledning til misforståelser, fordi $(\mathbb{N},+)$ og $(\tilde{\mathbb{N}},\tilde{+})$ har samme algebraiske struktur. Derefter er der ingen særlig grund til at operere med to forskellige kompositioner + og $\tilde{+}$, hvorfor vi simpelthen taler om $(\mathbb{Z},+)$ og om $(\mathbb{N},+)$ som en delmængde af $(\mathbb{Z},+)$.

Vi slutter dette afsnit med at foretage en opdeling af de hele tal i tre disjunkte delmængder.

Først vedtager vi i $(\mathbb{Z},+)$ at betegne det inverse til m med $-m$, og det neutrale element i gruppen med o. Derefter påstår vi:

Om ethvert element $a \in \mathbb{Z}$ gælder, at enten er $a = o$, eller $a \in \mathbb{N}$, eller $-a \in \mathbb{N}$, og at disse tilfælde er gensidigt udelukkende.

Dette indses således: Til a findes $m,n \in \mathbb{N}$, så at $a = m-n$. Hvis ikke $a = o$, svarende til at $m = n$, findes i følge Sætning I.14 i Kapitel I enten 1) et $x \in \mathbb{N}$, så at $n+x = m$, eller 2) et $x \in \mathbb{N}$, så at $m+x = n$, og ikke begge. Hvis det er 1) der gælder, er $x = n-m$, og dermed vil $a \in \mathbb{N}$, da $a = x \in \mathbb{N}$. Hvis 2) gælder, er $x = n-m = -a$, hvorved $-a \in \mathbb{N}$, da $x \in \mathbb{N}$. Dette viser, at én af de tre muligheder foreligger. At de er gensi-



Husk, at vi ikke uden videre i lettelse over nu at måtte tale om de hele tal, kan tillægge dem egenskaber, vi tror de har, men som ikke er etableret som sætninger. Egenskaberne må stables på benene fra bunden.

Om ordningen: Vi har ikke automatisk givet en ordning på de hele tal. Den må defineres, og det på en sådan måde, at den 1) udvider ordningen fra de naturlige tal,2) kun i udvidelsen benytter egenskaber ved de naturlige tals ordning som er konstateret under den aksiomatiske opbygning, og 3) opfylder de krav vi venter af den.

Tager vi udgangspunkt i 3) må en fornuftig ordning > på ℤ have egenskaben: $u > v \Leftrightarrow u-v \in \mathbb{N}$. Vi forsøger derfor at stange dette ud som definition, i håb om at de fornødne egenskaber så kommer i hus.

Læg mærke til, at harmoniegenskaben (b) uafladeligt benyttes i det følgende, når der drages slutninger om ordningen.

I øvrigt kaldes en irrefleksiv ordning <u>trichotymisk</u>, hvis det om to vilkårlige elementer u og v gælder, at enten er u = v, eller u > v eller v > u.

digt udelukkende, følger dels af at $o \notin \mathbb{N}$, hvilket forhindrer, at det første tilfælde kan forenes med noget af de to andre, dels af, at hvis $a \in \mathbb{N}$ og $-a \in \mathbb{N}$, ville $o = a+(-a) \in \mathbb{N}$, atter i strid med at $o \notin \mathbb{N}$.

Dette betyder, at vi kan fremstille ℤ som disjunkt forening af følgende tre mængder:

$$\mathbb{Z} = \{a \in \mathbb{Z} \setminus \{o\} \mid -a \in \mathbb{N}\} \cup \{o\} \cup \{a \in \mathbb{Z} \setminus \{o\} \mid a \in \mathbb{N}\}$$

Vi kalder elementerne i $\{a \in \mathbb{Z} \setminus \{o\} \mid a \in \mathbb{N}\}$ for <u>de positive</u> hele tal, og elementerne i $\{a \in \mathbb{Z} \setminus \{o\} \mid -a \in \mathbb{N}\}$ for <u>de negative</u> hele tal.

<u>Udvidelsen af de naturlige tals ordning til en ordning på de hele tal</u>

Vi definerer en ordning $>_{\mathbb{Z}}$ på følgende måde:

<u>Definition</u>: For u,v i ℤ defineres <u>relationen</u> $>_{\mathbb{Z}}$ ved

(7) $u >_{\mathbb{Z}} v \Leftrightarrow u-v \in \mathbb{N}$.

Vi ønsker at indse, at den således definerede relation er en total ordningsrelation, der udvider den tidligere indførte ordning (her for et øjeblik betegnet $>_{\mathbb{N}}$) på de naturlige tal, og at den på passende måde harmonerer med + i ℤ. Dette udtrykkes af

<u>SætningII.2</u>. Den ved (7) definerede relation er en <u>irrefleksiv ordningsrelation</u> med følgende egenskaber, samt trichotymi

(a) $\forall\, u,v \in \mathbb{N}: u >_{\mathbb{Z}} v \Leftrightarrow u >_{\mathbb{Z}} v$

(b) $\forall\, u,v,z \in \mathbb{Z}: u >_{\mathbb{Z}} v \Leftrightarrow u+z >_{\mathbb{Z}} v+z$.

<u>Beviset</u> består af en række simple efterprøvninger:

At relationen er trichotymisk ses umiddelbart af definitionen og opspaltningen af ℤ, jfr. ovenfor. At den er irrefleksiv skyldes at $o \notin \mathbb{N}$. At den endvidere er asymmetrisk ses således:

Lad $u >_{\mathbb{Z}} v$ og $v >_{\mathbb{Z}} u$. Så vil $u-v \in \mathbb{N}$ og $v-u \in \mathbb{N}$. Men så må $o = (u-v) + (v-u) \in \mathbb{N}$, i strid med at $o \notin \mathbb{N}$.

Transitiviteten er lige så enkel: Hvis $u >_{\mathbb{Z}} v$ og $v >_{\mathbb{Z}} z$, vil både $u-v \in \mathbb{N}$ og $v-z \in \mathbb{N}$. Men så vil også $u-z = (u-v)+(v-z)$ tilhøre ℕ.

Det ville jo være pinligt, hvis det ikke forholdt sig sådan. På den anden side følger det ikke af sig selv, der skal et argument til.

Ad (a): I følge definitionen af ordningen i $\mathbb{N}$ gælder om $>_{\mathbb{N}}$, for $u,v \in \mathbb{N}$:

(8) $u >_{\mathbb{N}} v \Leftrightarrow \exists p \in \mathbb{N}: u = v+p.$

Betingelsen (7) kan også udtrykkes - for $u,v \in \mathbb{Z}$:

(9) $u >_{\mathbb{Z}} v \Leftrightarrow \exists p \in \mathbb{N}: u = v+p.$

Af (8) og (9) ses, at for $u,v \in \mathbb{N}$ stemmer de to ordningsrelationer overens. Således er (a) bevist.

Ad (b): Vi har

$u >_{\mathbb{Z}} v \Leftrightarrow u-v \in \mathbb{N} \Leftrightarrow (u+z)-(v+z) = u-v \in \mathbb{N} \Leftrightarrow u+z >_{\mathbb{Z}} v+z,$

hvilket beviser (b) og dermed sætningen.

På grund af, at $>_{\mathbb{Z}}$ er en udvidelse af $>_{\mathbb{N}}$ i følge (a), skriver vi i fremtiden kun $>$ for dem begge.

Den tilsvarende refleksive ordningsrelation $\geq$ defineres ved

(10) $u \geq v \quad u > v$ eller $u = v$,

der for $u,v \in \mathbb{N}$ ses at stemme overens med den i kapitel I definerede refleksive ordningsrelation i $\mathbb{N}$. Desuden gælder den til Sætning II, (b) svarende egenskab med $\geq$ i stedet for $>$.

Det ses i øvrigt, jfr. side74, at $a \in \mathbb{Z}$ er et positivt helt tal, hvis og kun hvis $a > o$, og et negativt helt tal hvis og kun hvis $a < o$.

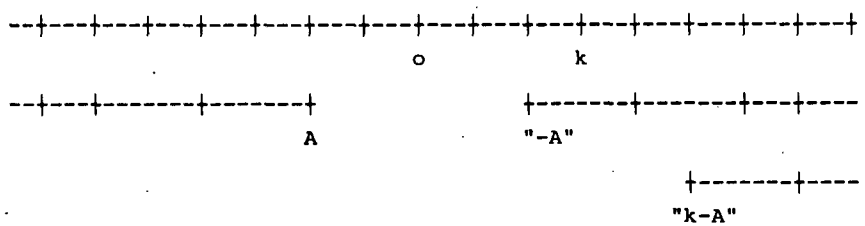
Til forskel fra mængden af naturlige tal er mængden af hele tal ikke velordnet ved $<$. F.eks. findes der ikke noget mindste element i mængden af negative hele tal. Hvis nemlig $m \in \mathbb{Z}$ er $m-1 < m$.

Der gælder imidlertid

Sætning II.3. Enhver opad begrænset ikke-tom delmængde af $\mathbb{Z}$ har et største element. Enhver nedad begrænset ikke-tom delmængde af $\mathbb{Z}$ har et mindste element.

Bevis. Lad $A \subseteq \mathbb{Z}$ være opad begrænset. Det indebærer, at der findes et $k \in \mathbb{Z}$, så at

Idéen i beviset er meget enkel: Det vi har hold over, er delmængder af $\mathbb{N}$, der jo er velordnet. Sådanne delmængder har - hvis de er ikke-tomme - altid et mindste element. Idéen består så i sammen med den givne mængde A, delmængde af $\mathbb{Z}$, at betragte en af A på naturlig måde fremgået delmængde B af $\mathbb{N}$. Mængden B har et mindste element, hvilket udnyttes til at indse, at A har et største element, hvis den er opad begrænset, og et mindste element, hvis den er nedad begrænset. For den del af beviset som bringes udførligt, kan B anskues (se figur) som den mængde der fremkommer ved at A spejles om o og derefter parallelforskydes ved k, altså uformelt skrevet B = k-A = -A+k.



For den del af beviset som kun antydes, kan B anskues (tegn selv figur) som A-m, dvs. den mængde der fremkommer af A ved parallelforskydningen -m.

$\forall a \in A: a < k$.

Så vil mængden

$$B = \{k-a \mid a \in A\}$$

være en delmængde af $\mathbb{N}$, idet jo for alle $a \in A$, $k-a > o$.

Da $\mathbb{N}$ er velordnet, og da B er ikke-tom, findes et mindste element i B. Lad dette være $k-a_o$, hvor $a_o \in A$. Nu er så a_o største element i A. Thi at $a_o \in A$ er allerede klart, og at for ethvert $a \in A$

$$a \leq a_o$$

følger af, at $k-a \in B$, hvorved

$$k-a \geq k-a_o.$$

I kraft af Sætning II.2. (b) er dette ensbetydende med, at $-a \geq -a_o$. Adderes hertil $a+a_o$ fås det ønskede.

Beviset for, at enhvert ikke-tom nedad begrænset delmængde A af $\mathbb{Z}$ har et mindste element, gennemføres analogt, ved at man - hvis m er et undertal for A - betragter mængden

$$\{a-m \mid a \in A\}.$$

<u>Udvidelse af multiplikationen i de naturlige tal til en multiplikation i de hele tal</u>.

For at have færdiggjort opbygningen af strukturen på de hele tal mangler vi at indføre en multiplikation. Denne multiplikation skal defineres sådan, at den er en udvidelse af den multiplikation der tidligere er indført på de naturlige tal.

Til brug for indførelsen af en multiplikation på $\mathbb{Z}$ benytter vi, at ethvert helt tal i følge Sætning II.1 (punkt (2)) kan fremstilles som en differens mellem to naturlige tal. Hvis derfor g_1 og g_2 er to vilkårlige hele tal, findes m_1, n_1 og m_2, $n_2 \in \mathbb{N}$, så at

$$g_1 = m_1 - n_1 \text{ og } g_2 = m_2 - n_2.$$

Eftersom vi ønsker at den søgte multiplikation - lad os i begyndelsen betegne den med $\tilde{\cdot}$ -skal være distributiv med hensyn til +,

Vi skal vise, at hvis $m_1-n_1 = m_1'-n_1'$ og $m_2-n_2 = m_2'-n_2'$ er
$(m_1m_2+n_1n_2)-(m_1n_2+m_2n_1) = (m_1'm_2'+n_1'n_2')-(m_1'n_2'+m_2'n_1')$.
Ved omordning ses, at dette kommer ud på at vise, at hvis

(a) $m_1+n_1' = m_1'+n_1$ og (b) $m_2+n_2' = m_2'+n_2$

er

(c) $m_1m_2+n_1n_2+m_1'n_2'+m_2'n_1' = m_1'm_2'+n_1'n_2'+m_1n_2+m_2n_1$.

At vise (c) kommer ud på at vise den identitet der fremgår af (c) ved at addere

$m_1n_2'+n_1m_2'+m_1'm_2+n_2n_1'$ (lig $n_1m_2'+m_1n_2'+n_2n_1'+m_1'm_2$)

til begge sider af lighedstegnet. Vi skal altså vise identiteten

$(m_1m_2+n_1n_2+m_1'n_2'+m_2'n_1')+(m_1n_2'+n_1m_2'+m_1'm_2+n_2n_1') =$
$(m_1'm_2'+n_1'n_2'+m_1n_2+m_2n_1)+(n_1m_2'+m_1n_2'+n_2n_1'+m_1'm_2)$.

Nu er venstresiden lig

$m_1(m_2+n_2')+n_1(n_2+m_2')+m_1'(n_2'+m_2)+n_1'(m_2'+n_2) =$
$m_1(m_2'+n_2)+n_1(n_2+m_2')+m_1'(n_2+m_2')+n_1'(m_2'+n_2) =$
$(m_2'+n_2)(m_1+n_1+m_1'+n_1') = (m_2'+n_2((m_1+n_1')+(n_1+m_1')) = 2(m_2'+n_2)(m_1+n_1')$,

hvor det første lighedstegn følger af en omformning af den første og den tredje parentes ved hjælp af (b), mens det tredje lighedstegn fremgår ved omformning af andet led ved hjælp af (a).

Højresiden omformes efter samme principper til

$2(m_1+n_1')(m_2'+n_2)$.

Da det heraf fremgår, at højresiden stemmer overens med venstresiden, er identiteten vist.

må den opfylde

$$g_1 \tilde{\cdot} g_2 = (m_1 - n_1)\tilde{\cdot}(m_2 - n_2)$$
$$= (m_1\tilde{\cdot}m_2 + n_1\tilde{\cdot}n_2) - (n_1\tilde{\cdot}m_2 + m_1\tilde{\cdot}n_2),$$

og eftersom vi desuden ønsker, at multiplikationen for naturlige tal skal stemme overens med den på $\mathbb{N}$ givne, må vi have

$$g_1 \tilde{\cdot} g_2 = (m_1m_2 + n_1n_2) - (m_1n_2 + m_2n_1).$$

Vi tager udgangspunkt i disse overvejslser i lanceringen af følgende formelle definition:

Definition. Der defineres en komposition $\tilde{\cdot}$ i $\mathbb{Z}$ således:
Lad g_1 og g_2 være vilkårlige elementer i $\mathbb{Z}$, og lad m_1, n_1 og m_2, $n_2 \in \mathbb{N}$ være valgt således, at

$$g_1 = m_1 - n_1 \text{ og } g_2 = m_2 - n_2.$$

Så sættes

(11) $$g_1 \tilde{\cdot} g_2 = (m_1m_2 + n_1n_2) - (m_1n_2 + m_2n_1).$$

For at man overhovedet kan tale om en definition i denne sammenhæng, må det godtgøres, at hvis

$$g_1 = m_1' - n_1' \text{ og } g_2' = m_2' - n_2'$$

er andre fremstillinger af g_1 og g_2, hvor m_1', n_1' og m_2', n_2' er i $\mathbb{N}$, bliver

$$(m_1m_2 + n_1n_2) - (m_1n_2 + m_2n_1) = (m_1'm_2' + n_1'n_2') - (m_1'n_2' + m_2'n_1').$$

Beviset for dette er elementært, men lidt tungt, og præsenteres på side 79.

Dernæst skal vi indse, at $\tilde{\cdot}$ er en udvidelse af $\cdot$ fra $\mathbb{N}$.

Lad til den ende $m, n \in \mathbb{N}$. Så er, for $p,q \in \mathbb{N}$
$m = (m+p)-p$ og $n = (n+q)-q$
fremstillinger af henholdsvis m og n på formen (2) i Sætning II.1, hvorfor i følge (11):

$$m \tilde{\cdot} n = ((m+p)-p)\tilde{\cdot}((n+q)-q) = (m+p)(n+q)+pq-((m+p)q+(n+q)p)$$
$$= mn+pn+mq+pq-mq-pq-np-qp = mn.$$

Der er nu ikke længere grund til at opretholde et særligt tegn $\tilde{\cdot}$ for multiplikationen i $\mathbb{Z}$. Vi skriver for fremtiden blot $\cdot$, og når det er bekvemt uv i stedet for u·v.

Vi er stadig nødt til at bevise disse fra et dagligdags synspunkt trivielle egenskaber fra grunden.

At $\cdot$ er kommutativ og associativ samt distributiv med hensyn til + er let at vise. Det ses ved regulær udregning på grundlag af (11).

Tallet 1 er neutralt element ved $\cdot$, idet for $g = m-n$ og med observationen $1 = (1+p)-p$ fås

$$1\cdot g = ((1+p)m + pn) - ((1+p)n + mp) = m+pm+pn-n-pn-mp$$
$$= m-n = g.$$

Desuden er $o\cdot g = o$, thi

$$o\cdot g = (p-p)\ (m-n) = pm+pn-(pn+mp) = o.$$

Og $(-g)h = g(-h) = -gh$, idet vi af

$$o = oh = (g+(-g))h = gh + (-g)h$$

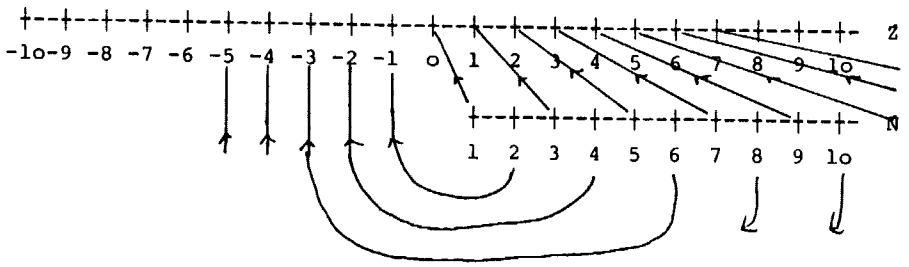
slutter, at $(-g)h = -gh$, og dermed at $g(-h) = (-h)g = -hg = -gh$.

Nulreglen gælder i $\mathbb{Z}$:

Hvis $gh = o$, er $g = o$ eller $h = o$.

Thi: idet $m_1, n_1, m_2, n_2 \in \mathbb{N}$, og
$g = m_1 - n_1$ og $h = m_2 - n_2$,
er $gh = o$ ensbetydende med, at
$o = (m_1 - n_1)(m_2 - n_2) = m_1m_2 - n_1m_2 - m_1n_2 + n_1n_2$
$= m_1m_2 + n_1n_2 - (n_1m_2 + m_1m_2)$,
der igen er ensbetydende med, at
$m_1m_2 + n_1n_2 = n_1m_2 + m_1n_2$.
Er nu $g = o$ er påstanden øjensynlig rigtig. Hvis ikke, dvs, hvis $g \neq o$, er enten $g \in \mathbb{N}$ eller $-g \in \mathbb{N}$. Antager vi først at $g \in \mathbb{N}$, findes et $q \in \mathbb{N}$, $q \neq o$, så at
$m_1 - n_1 = q$, dvs. $m_1 = q + n_1$.
Det betyder, at forudsætningen $gh = o$ kan udtrykkes
$(q + n_1)m_2 + n_1n_2 = n_1m_2 + (q + n_1)n_2$,
der ved omskrivning ses at være ensbetydende med, at
$qm_2 + n_1m_2 + n_1n_2 = n_1m_2 + qn_2 + n_1n_2$.
Men eftersom forkortningsreglerne gælder for addition i $\mathbb{N}$ kommer den sidste identitet ud på at
$qm_2 = qn_2$.
Benyttes herefter forkortningsreglen for multiplikation i $\mathbb{N}$ ses, idet $q \neq o$, at $m_2 = n_2$, hvilket udtrykker, at $h = m_2-n_2=o$.

Afbildningen f kan illustreres således



Argumentationen i tilfældet $-g \in \mathbb{N}$ forløber parallelt.

Når nulreglen gælder i $\mathbb{Z}$ gælder for multiplikationen den modificerede forkortningsregel, der siger at faktorer forskellige fra o kan bortforkortes.

For at få afrundet billedet af de hele tal mangler vi et par ting. Først en undersøgelse af, hvordan ordningen spiller sammen med multiplikationen:

Sætning II.4. For vilkårlige elementer g,h,u,v i $\mathbb{Z}$ gælder
(12) $g < h$ og $o < v \Rightarrow gv < hv$
(13) $g \leq h$ og $o \leq v \Rightarrow gv \leq hv$.

Bevis. Vi viser først (12):
Forudsætningerne $g < h$ og $o < v$ kan udtrykkes $h-g \in \mathbb{N}$ og $v \in \mathbb{N}$.
Heraf følger, at $hv - gv = (h-g)v \in \mathbb{N}$,
hvorfor $gv < hv$.

Hvad (13) angår har vi: Hvis $g = h$ er $gv = hv$ og dermed $gv \leq hv$.
Hvis $o = v$ er $gv = go = o = hv$, og dermed atter $gv \leq hv$. De øvrige tilfælde falder ind under (12). Q.E.D.

De fundne egenskaber om de hele tal kan opsummeres således:

$(\mathbb{Z},+,\cdot,<)$ er en kommutativ integritetsring med ételement, med en ordning, der harmonerer med kompositionerne. Enhver opad (nedad) begrænset, ikke-tom delmængde af $\mathbb{Z}$ har en største (mindste) element.

Vi slutter med:

Sætning II.5. $\mathbb{Z}$ er ækvipotent med $\mathbb{N}$

Bevis.

Funktionen $f: \mathbb{N} \sim \mathbb{Z}$, defineret ved

$$f(n) = \begin{cases} p, \text{ hvis } n \text{ er ulige og har formen } n = 2p+1,\ p \in \mathbb{N} \\ o, \text{ hvis } n = 1 \\ -p, \text{ hvis } n \text{ er lige og har formen } n = 2p,\ p \in \mathbb{N} \end{cases}$$

er bijektiv. At den er injektiv følger således: hvis $f(n) = f(m)$ kan det ikke tænkes, at det om m og n gælder, at den ene er lige, mens den anden er ulige. Thi f's værdi på et lige tal er ne-

Hvis noget af det følgende forekommer uigenneskueligt, så tænk på det specialtilfælde, hvor p = 10!

Med denne konvention kan vi i stedet for c_o skrive $c_o p^o$. ⟶

gativ, mens dens værdi på ulige tal er ikke-negativ. Vi har altså, at m og n enten begge er lige eller begge er ulige. I det første tilfælde har m og n formen henholdsvis m = 2p og n = 2q, og dermed p = f(m) = f(n) = q. Men så er m = 2p = 2q = n. Er m og n begge ulige, af formen m = 2p+1 og n = 2q+1, er -p = f(m) = f(n) = -q, hvorved p = q, og derfor m = n. Dette ræsonnement viser, at f er injektiv.

Surjektiviteten af f følger således: Lad u være et vilkårligt helt tal. Så er u enten ikke-negativt eller negativt. Hvis u er ikke-negativt, er n = 2u+1 et naturligt, ulige tal. Hvis u = o, er n = 1 og f(1) = o = u. Hvis u > o, dvs. u ∈ ℕ, er f(n) = u. Er u negativt, er n = 2(-u) et lige, naturligt tal. Derfor er f(n) = -(-u) = u. I alle tilfælde er u indfanget som billede ved f af et naturligt tal. Men så er f surjektiv. Q.E.D.

*

Positionssystemer i ℕ

Med de hele tal får vi tallet o til rådighed. Vi er dermed i stand til at afvikle hængepartiet fra Kapitel I: at indføre positionssystemer i mængden af naturlige tal. Det sker gennem denne sætning:

Sætning II.6. Ethvert naturligt tal p ≠ 1 kan tjene som grundtal for et positionssystem i ℕ. Det betyder, at ethvert naturligt tal n på netop én måde kan fremstilles på formen

(14) $n = c_k p^k + c_{k-1} p^{k-1} + \ldots + c_1 p^1 + c_o$,

for et eller andet $k \in \mathbb{N} \cup \{o\}$, og med koefficienter $c_i \in \mathbb{N}$, $o \leq c_i \leq p-1$, $i = o,\ldots,k$, $c_k > o$. Vi bruger også skrivemåden

$$n = c_k c_{k-1} \cdots c_1 c_o.$$

Bevis: Allerførst skal vi sikre os, at der er mening i at tale om de indgående potenser. Den sikring får vi af rekursionssætningen med A = ℕ, a = p og funktionen g: A ⟶ A defineret ved g(x) = p·x. Desuden sættes $p^o = 1$.

Denne ulighed er baseret på at ethvert $d_i \leq p-1$ $(i=1,\ldots m)$, og på at uligheder mellem hele tal bevares efter multiplikation med positive hele tal, her p^i. (At p^i er positiv følger af den samme bevarelsesegenskab og et let induktionsræsonnement (gennemfør det selv!)) Hvis man var overmåde pedantisk, skulle også den efterfølgende udregning bekræftes af et induktionsbevis.

Uligheden $p^{m+1} \leq p^k$ følger (ved induktion) af at $p > 1$, og af at $m+1 \leq k$, når $m < k$. Uligheden $p^k \leq c_k p^k$ følger af at $c_k > 0$ og $p^k \geq 0$.

Uligheden følger af at for alle i gælder $p-1 \geq d_i \geq d_i - c_i$, hvorved $(c_i - d_i) \geq -(p-1)$, og videre

$$(c_i - d_i)p^i \geq -(p-1)p^i.$$

Dernæst viser vi sætningens entydighedspåstand. Lad os antage, at n havde to forskellige fremstillinger af formen (14):

(*) $n = c_k p^k + c_{k-1} p^{k-1} + \ldots + c_1 p^1 + c_0$

og

(**) $n = d_m p^m + d_{m-1} p^{m-1} + \ldots + d_1 p^1 + d_0$.

Det må nu først gælde, at $k = m$. Ellers var k ellerm størst, f.eks. $k > m$. Men da

$$\begin{aligned} n &= d_m p^m + d_{m-1} p^{m-1} + \ldots + d_1 p^1 + d_0 \\ &\leq (p-1)p^m + (p-1)p^{m-1} + \ldots + (p-1)p + (p-1) \\ &= p^{m+1} + p^m + \ldots + p^2 + p - p^m - p^{m-1} - \ldots - p - 1 \\ &= p^{m+1} - 1 < p^{m+1} \leq p^k \leq c_k p^k \leq c_k p^k + c_{k-1} p^{k-1} + \ldots + c_1 p^1 + c_0 \\ &= n \end{aligned}$$

På grund af det skarpe ulighedstegn i næstsidste linje er altså $n < n$, hvilket er i modstrid med ordningen i de naturlige tal.

Vi kan altså ikke have, at $k > m$. På tilsvarende måde aflives muligheden $k < m$. Derfor er $k = m$.

Det har til følge, at fremstillingerne (*) og (**) antager formen

(*) $n = c_k p^k + c_{k-1} p^{k-1} + \ldots + c_1 p^1 + c_0$

og

(**) $n = d_k p^k + d_{k-1} p^{k-1} + \ldots + d_1 p^1 + d_0$.

Vi skal nu indse, at alle koefficienterne i (*) og i (**) stemmer overens, altså at $c_i = d_i$ for $i = 0,1,\ldots k$.

Lad os antage, at dette ikke er tilfældet. Så må der være et største nummer $s \in \{0,1,\ldots k\}$, for hvilket $c_s \neq d_s$. Lad $c_s > d_s$. (Hvis den modsatte ulighed holder ræsonneres helt parallelt). Subtraheres (**) fra (*) fås:

$$\begin{aligned} 0 &= (c_k - d_k)p^k + \ldots + (c_{s+1} - d_{s+1})p^{s+1} + (c_s - d_s)p^s + \ldots + (c_0 - d_0) \\ &= (c_s - d_s)p^s + \ldots + (c_1 - d_1)p^1 + (c_0 - d_0) \\ &\geq (c_s - d_s)p^s - (p-1)p^{s-1} - \ldots - (p-1)p - (p-1) \end{aligned}$$

$$= (c_s-d_s)p^s-p^s-\ldots-p^2-p+p^{s-1}+\ldots+p+1$$

$$= (c_s-d_s)p^s-p^s+1 = (c_s-d_s-1)p^s+1$$

$$\geq 0\cdot p^s+1 = 1,$$

idet $c_s > d_s$ medfører, at $c_s \geq d_s+1$. Men uligheden $0 \geq 1$ er ikke korrekt i $\mathbb{Z}$. Antagelsen om at c'erne og d'erne er forskellige kan altså ikke opretholdes. Men så er de to sæt ens, og entydigheden er bevist.

Tilbage står at bevise eksistenspåstanden. Det foregår ved induktion. Vi danner mængden

$$M = \{n \in \mathbb{N} \mid \text{der findes et } k \in \mathbb{N} \cup \{0\} \text{ og koefficienter } c_0,\ldots c_k \in \{0,1\ldots p-1\}, c_k \neq 0 \text{, så at } n = c_k p^k+\ldots c_1 p^1+c_0\}$$

Først skal vi godtgøre, at $1 \in M$. Men det er trivielt, da for $k = 0$ og $c_0 = 1$, $1 = c_0$.

Dernæst går vi ud fra, at $n \in M$, og skal så vise at $S(n) = n+1 \in M$. Når $n \in \mathbb{N}$ findes en fremstilling

$$n = c_k p^k+\ldots+c_1 p^1+c_0$$

med et passende $k \in \mathbb{N} \cup \{0\}$ og med passende koefficienter $c_0,\ldots c_k$. Der er nu to muligheder. Enten (1) er alle koefficienter $c_0,\ldots c_k$ lig p-1, eller (2) der findes en koefficient blandt c'erne som ikke er p-1.

Lad os betragte mulighed (1) først. Vi har da

$$n = (p-1)p^k+(p-1)p^{k-1}+\ldots+(p-1)p+(p-1)$$

$$= p^{k+1}+p^k+\ldots+p-p^k-p^{k-1}-\ldots-p-1$$

$$= p^{k+1}-1.$$

Men så er $n+1 = p^{k+1}$, hvilket er en fremstilling af n+1 på den ønskede form (med k+1 i stedet for k og med $(c_0,\ldots c_{k+1}) = (0,\ldots 0,1)$)

(2) Hvis der, dernæst, findes en koefficient som ikke er p-1, må der findes et mindste nummer i, så at $c_i \neq p-1$, hvoraf $c_i \leq p-2$. Det betyder at n har fremstillingen

Den sidste fremstilling kan benyttes, hvis allerede $c_o \neq p-1$. Den første anvendes, hvis dette ikke er tilfældet. Hvis $i = 1$ er der i denne fremstilling kun leddet $p-1$ til højre for $c_i p^i$.

$$n = \begin{cases} c_k p^k + \ldots + c_i p^i + (p-1)p^{i-1} + \ldots + (p-1), & \text{hvis } i \geq 1 \\ c_k p^k + \ldots + c_1 p^1 + c_o, & \text{hvis } i = o. \end{cases}$$

Og dermed n+1 fremstillingen

$$n+1 = \begin{cases} c_k p^k + \ldots + c_i p^i + p^i + \ldots + p^2 + p - p^{i-1} - \ldots - p - 1 + 1 \\ = c_k p^k + \ldots + c_i p^i + p^i = c_k p^k + \ldots + c_{i+1} p^{i+1} + (c_i + 1)p^i \quad (a) \\ c_k p^k + \ldots + c_1 p^1 + (c_o + 1) \quad (b). \end{cases}$$

Uanset om $i = o$ eller $i \geq 1$, vil $(c_i+1) \in \{o,1 \ldots p-1\}$, eftersom $c_i \leq p-2$. Det bevirker, at n+1 har en fremstilling af den ønskede art. I tilfælde (b) står den der umiddelbart. I tilfælde (a) fremkommer den ved tilføjelse af leddet $o \cdot p^{i-1} + \ldots + o$. I alt er $n+1 \in M$, og induktionsbeviset er fuldført. Q.E.D.

III. DE RATIONALE TAL.

Udvidelse af de hele tal til de rationale tal

Uformel indledning

Skønt mængden af hele tal, ved at udgøre en ordnet kommutativ integritetsring med ételement, er forsynet med en struktur, der tillader løsning af en lang række opgaver, lider den af den mangel at divisionsopgaver kun "sjældent" lader sig løse. Grunden er at kun ételementet og dets modsatte har et inverst ved multiplikation.

Vi spørger derfor: Kan vi foretage en udvidelse af mængden af hele tal til en algebraisk struktur, hvori også (næsten) enhver divisionsopgave kan løses, og som i øvrigt har de egenskaber som er gældende for de hele tal? Vores ønske er desuden at foretage en så "lille" udvidelse som muligt, dvs. således at der ikke findes en "mindre" mængde omsluttende $\mathbb{Z}$, som har de efterspurgte egenskaber. Spørgsmålet kan i en lidt mere teknisk udgave formuleres således: Findes der et mindste kommutativt legeme der omfatter $\mathbb{Z}$?

Division er principielt en sag mellem to tal, til hvilke man knytter et tredje, resultatet af divisionen. Hvis de to tal, u og v, der er i betragtning, er naturlige tal, hvor v går op i u, er divisionen af u med v mulig, og resultatet er et naturligt tal. Vi kan sige at parret (u,v) repræsenterer resultatet af divisionen, idet vi selvsagt underforstår at repræsentationen skal ske i forhold til divisionsbegrebet.

Parallelt hertil kan vi også repræsentere "divisioner som ikke går op" med parret af "dividend" og "divisor".

Det næste skridt bliver at organisere mængden af par af hele tal, hvis anden-komponent er forskellig fra o, med den tanke i baghovedet, at parrene ved organiseringen skal agere ligesom brøker gør det i hverdagen. Det bliver her - ligesom ved udvidelsen af de naturlige tals mængde til de hele tals mængde - påkrævet at regne sådanne par for ækvivalente, som i brøkhenseende

er ens. Et umiddelbart bud er at identificere (u,v) med (p,q) hvor og kun hvis uq = pv. Dette vil da også blive gjort i det følgende.

Vi kunne godt have valgt en lidt anderledes fremgangsmåde i opbygningen af de rationale tal. Tager vi nemlig udgangspunkt i den observation, at $(\mathbb{N},\cdot)$ er en kommutativ semigruppe hvori forkortningsreglerne gælder, kan vi med en konstruktion helt parallel med den vi benyttede til at danne $(\mathbb{Z},+)$ ud fra $(\mathbb{N},+)$ udvide $(\mathbb{N},\cdot)$ til en kommutativ semigruppe, der faktisk ville vise sig at blive $(\mathbb{Q}_+,\cdot)$, altså de positive rationale tal forsynet med $\cdot$. Derefter kunne addition i $\mathbb{Q}_+$ defineres nogenlunde som der sker i dette kapitel. Det ville frembringe endnu en kommutativ semigruppe med forkortningsreglerne gældende. Den kunne derefter udvides til en gruppe $(\mathbb{Q},+)$, hvori også de negative rationale tal og o ville optræde. Tilbage ville så stå at udvide $\cdot$ til hele $\mathbb{Q}$ og at vise, at $(\mathbb{Q},+,\cdot)$ således konstrueret er et kommutativt legeme, der opfylder (i)-(iv) i Sætning III.1. En sådan fremfærd ville meget vel have været realiserbar, og ville endda svare bedre end den valgte til den første moderne konstruktion, udført af H. Weber i 1895. Arbejdets omfang er stort set det samme i de to fremgangsmåder, og valget må først og fremmest blive en smagssag. Når det er faldet ud som det er, skyldes det en fornemmelse af at med de hele tals integritetsring til rådighed vil det føles mest nærliggende straks at indføre alle rationale tal, og ikke først de positive.

Webers konstruktion ligger i forlængelse af tidligere bestræbelser på området. B. Bolzano betragtede (1831) i et efterladt skrift de rationale tal som en mængde der var afsluttet over for de fire regningsarter. Et sådant kaldte Kronecker et rationalitetsområde, Dedekind (1871) et legeme. Et helt abstrakt legemebegreb, frigjort fra bindinger til talområder, indførtes af Steinitz i 1910. Han viste også, at en vilkårlig kommutativ integritetsring kan udvides til et kommutativt legeme, det såkaldte udvidelseslegeme. Sætning III.1. er derved et specialtilfælde af en generel sætning om kommutative integritetsringes udvidelse.

Som i det foregående kapitel kunne der i selve formuleringen af sætningen have været grund til at skelne mellem kompositioner i $\mathbb{Z}$ og i L. Det antages imidlertid at det ikke længere er påkrævet. Derimod er der gennemført en skelnen undervejs i beviset, fordi så mange forskellige algebraiske strukturer er i spil samtidig.

Læg mærke til, at vi ikke starter med at indføre en komposition umiddelbart i P for derefter at overføre den til kvotientmængden. Den komposition der om lidt indføres defineres direkte på kvotientmængden.

Udvidelsen af de hele tal til de rationale tal

Resultatet af vore bestræbelser tager form af følgende sætning:

Sætning III.1. Der findes et kommutativt legeme $(L,+,\cdot)$ med følgende egenskaber

i) Der findes en delmængde M af L, så at $(M,+,\cdot)$ er en kommutativ integritetsring indeholdende ételementet i L, og så at $(\mathbb{Z},+,\cdot)$ er isomorf med $(M,+,\cdot)$.

ii) Ethvert element $r \in L$ kan fremstilles på formen
(1) $r = uv^{-1}$
for et $u \in M$ og et $v \in M \setminus \{o\}$.

iii) $(L,+,\cdot)$ er i følgende forstand det mindste kommutative legeme, der har $(\mathbb{Z},+,\cdot)$ som delring:
Hvis $(L',+,\cdot)$ er et kommutativt legeme, der har $(\mathbb{Z},+,\cdot)$ som delring (i samme betydning som i i)) findes et dellegeme af $(L',+,\cdot)$, som er isomorft med $(L,+,\cdot)$.

iv) Hvis $(L_1,+,\cdot)$ opfylder i) og ii) er $(L,+,\cdot)$ isomorft med $(L_1,+,\cdot)$.

Bevis:

Vi betragter mængden af par af hele tal, hvis anden-komponent er forskellig fra o. Altså

$$P = \mathbb{Z}x(\mathbb{Z} \setminus \{o\}) = \{(u,v) \mid u \in \mathbb{Z},\ v \in \mathbb{Z} \setminus \{o\}\}.$$

I P fastlægges en relation $\sim$ ved

(2) $(p,q) \sim (s,t) \Leftrightarrow pt = qs$.

Denne relation $\sim$ er en ækvivalensrelation:

$\sim$ er refleksiv, thi da $pq = qp$, er $(p,q) \sim (q,p)$.

$\sim$ er symmetrisk, thi hvis $(p,q) \sim (s,t)$, dvs. hvis $pt = qs$, er $sq = tp$ og dermed $(s,t) \sim (p,q)$.

$\sim$ er transitiv, thi hvis $(p,q) \sim (s,t)$ og $(s,t) \sim (u,v)$ er $pt = qs$ og $sv = tu$. Dermed er også $(pt)sv = (qs)tu$, eller anderledes udtrykt, $(ts)pv = (ts)qu$. Men så er $ts(pv - qu) = o$. Det bevirker, fordi nulreglen gælder i $\mathbb{Z}$, at $pv - qu = o$, eller at $ts = o$. Vi vil gerne indse, at $pv = qu$. Hvis $ts \neq o$ er umiddelbart $pv = qu$. Vi antager dernæst, at $ts = o$. Nu er $t \neq o$,

Hvis vi tænker på, at de forskellige par (u,v) fremkommer som en formel måde at indføre det der i vores baghovede skal være "brøker" (vi tænker altså på (u,v) som "u/v"), er det oplagt, at klassen indeholdende (u_1,v_1) (altså "brøken u_1/v_1") adderet til klassen indeholdende parret (u_2,v_2) (altså brøken u_2/v_2) må blive klassen der modsvarer brøken $(u_1/v_1)+(u_2/v_2)$, lig med brøken $(u_1v_2+v_1u_2/v_1v_2)$. Men det er jo netop klassen der indeholder parret $(u_1v_2+v_1u_2,v_1v_2)$.

idet $(s,t) \in P$. Derfor ville $ts = o$ medføre (på grund af nulreglen), at $s = o$. Men af $s = o$ følger:
$o = qs = pt$ og $o = sv = tu$, og dermed (da $t \neq o$), at $p = o$ og $u = o$. Men så er $pv = qu$.

Efter at vi hermed har indset, at $\sim$ er en ækvivalensrelation, betragter vi kvotientmængden $L = P/\sim$. Den klasse i L, hvis repræsentant er (u,v) betegnes med $\Lambda_{(u,v)}$.

Vi definerer en komposition + i L på følgende måde:

Lad Λ_1 og $\Lambda_2 \in L$. Så findes (u_1,v_1) og $(u_2,v_2) \in P$, så at

$$\Lambda_1 = \Lambda_{(u_1,v_1)} \text{ og } \Lambda_2 = \Lambda_{(u_2,v_2)}.$$

Vi sætter så

$$(3)\quad \Lambda_1 + \Lambda_2 = \Lambda_{(u_1,v_1)} + \Lambda_{(u_2,v_2)} = \Lambda_{(u_1v_2+v_1u_2,v_1v_2)}.$$

Som sædvanlig skal det godtgøres, at dette er en definition, dvs. at forskriften i (3) ikke afhænger af valget af repræsentanter. Først skal det dog konstateres, at $(u_1v_2+v_1u_2,v_1v_2) \in P$, hvilket er opfyldt, fordi $v_1 \neq o$ og $v_2 \neq o$ medfører (nulreglen gælder i Z), at $v_1v_2 \neq o$.

Hvis $(u_1',v_1') \in \Lambda_1$ og $(u_2',v_2') \in \Lambda_2$, vil $(u_1',v_1') \sim (u_1,v_1)$ (dvs. $u_1'v_1 = v_1'u_1$) og $(u_2',v_2') \sim (u_2,v_2)$ (dvs. $u_2'v_2 = v_2'u_2$).
Vi skal indse, at

$$(u_1'v_2'+v_1'u_2',v_1'v_2') \sim (u_1v_2+v_1u_2,v_1v_2).$$

Nu er

$$(u_1'v_2'+v_1'u_2')v_1v_2 = u_1'v_2'v_1v_2+v_1'u_2'v_1v_2 = (u_1'v_1)(v_2'v_2)+(u_2'v_2)(v_1'v_1).$$

Desuden er

$$v_1'v_2'(u_1v_2+v_1u_2) = v_1'v_2'u_1v_2+v_1'v_2'v_1u_2 = (v_1'u_1)(v_2'v_2)+(u_2v_2')(v_1v_1').$$

Hermed er det ønskede vist.

I det følgende vil det blive vist, at (L,+) er en kommutativ gruppe. At + er kommutativ er oplagt, fordi + og · er kommutative i Z. At + er associativ følger også let:

$$(\Lambda_{(u_1,v_1)} + \Lambda_{(u_2,v_2)}) + \Lambda_{(u_3,v_3)} = \Lambda_{(u_1v_2+v_1u_2,v_1v_2)} + \Lambda_{(u_3,v_3)}$$
$$= \Lambda_{((u_1v_2+v_1u_2)v_3+v_1v_2u_3,\ v_1v_2v_3)} = \Lambda_{(u_1v_2v_3+v_1u_2v_3+v_1v_2u_3,v_1v_2v_3)}$$

og

$$\Lambda_{(u_1,v_1)} + (\Lambda_{(u_2,v_2)} + \Lambda_{(u_3,v_3)}) = \Lambda_{(u_1,v_1)} + \Lambda_{(u_2v_3+v_2u_3,v_2v_3)}$$
$$= \Lambda_{(u_1v_2v_3+v_1(u_2v_3+v_2u_3),v_1v_2v_3)}.$$

Her skal man tænke på, at i vort baghovede er tallet "o" det samme som enhver brøk med tæller o.

Dette er ikke overraskende, når man tænker på $\Lambda_{(u,v)}$ som brøken u/v.

Ud fra lignende overvejelser som dem der lå bag forskriften for addition må produktet af den klasse der indeholder (u_1,v_1) (altså brøken u_1/v_1) og den klasse der indeholder (u_2,v_2) (altså brøken u_2/v_2) være den klasse, der indeholder brøken $(u_1/v_1)\cdot(u_2/v_2)$, som er lig med brøken $(u_1u_2)/(v_1v_2)$. Resultatet skal med andre ord blive klassen der indeholder parret (u_1u_2,v_1v_2).

Her skal man tænke på, at $\frac{v}{u}$ er/ skal være den omvendte til $\frac{u}{v}$. ⟶

Sættes $N = \Lambda_{(o,1)}$ ses, at for $v \neq o$ vil $(u,v) \in N$ hvis og kun hvis $(u,v) \sim (o,1)$, eller m.a.o, hvis og kun hvis $u = u\cdot 1 = o$. Således er $N = \{(o,v) \mid v \in \mathbb{Z} \setminus \{o\}\}$. Nu er N neutralt element ved +.

Thi $\Lambda_{(u,v)} + N = \Lambda_{(u,v)} + \Lambda_{(o,1)} = \Lambda_{(u\cdot 1+v\cdot o, v\cdot 1)} = \Lambda_{(u,v)}$.

Ethvert element i L har et inverst ved +. Det inverse til $\Lambda_{(u,v)}$ er nemlig $\Lambda_{(-u,v)}$.

Thi $\Lambda_{(u,v)} + \Lambda_{(-u,v)} = \Lambda_{(uv+v(-u),v^2)} = \Lambda_{(o,v^2)} = N$.

Alt i alt har vi hermed vist, at (L,+) er en kommutativ gruppe.

Dernæst indføres en komposition · i L ved at vi for vilkårlige Λ_1 og Λ_2 i L med repræsentanter henholdsvis (u_1,v_1) og (u_2,v_2) fra P sætter

(4) $\Lambda_1 \cdot \Lambda_2 = \Lambda_{(u_1,v_1)} \cdot \Lambda_{(u_2,v_2)} = \Lambda_{(u_1u_2,v_1v_2)}$.

Også dette har mening. Først og fremmest er $v_1v_2 \in \mathbb{Z} \setminus \{o\}$.

Dernæst kan man af $(u_1',v_1') \sim (u_1,v_1)$ (dvs. $u_1'v_1 = v_1'u_1$) og $(u_2',v_2') \sim (u_2,v_2)$ (dvs. $u_2'v_2 = v_2'u_2$) slutte, at $(u_1'u_2',v_1'v_2') \sim (u_1u_2,v_1v_2)$, idet $u_1'u_2'v_1v_2 = u_1'v_1u_2'v_2 = v_1'u_1v_2'u_2 = v_1'v_2'u_1u_2$.

Nu er $(L \setminus \{N\},\cdot)$ en kommutativ gruppe. Thi, at $L \setminus \{N\}$ er stabil over for · er klart,

da for $u_1 \neq o$ og $u_2 \neq o$ $u_1u_2 \neq o$, og dermed $\Lambda_{(u_1,v_1)} \cdot \Lambda_{(u_2,v_2)} = \Lambda_{(u_1u_2,v_1v_2)} \neq N$.

Kommutativiteten af · er oplagt.

Sætter vi $E = \Lambda_{(1,1)}$ ses, at $(u,v) \in E \Leftrightarrow (u,v) \sim (1,1)$, eller m.a.o. $\Leftrightarrow u = v$. Altså er $E = \{(w,w) \mid w \in \mathbb{Z} \setminus \{o\}\}$ og $E \in L \setminus \{N\}$. E er neutralt element i $(L \setminus \{N\},\cdot)$,

thi for $\Lambda_{(u,v)} \in L \setminus \{N\}$ er $\Lambda_{(u,v)}\cdot E = \Lambda_{(u,v)} \cdot \Lambda_{(1,1)} = \Lambda_{(u,v)}$.

Ethvert element i $(L \setminus \{N\},\cdot)$ har et inverst element.

For $\Lambda_{(u,v)} \in L \setminus \{N\}$ er nemlig $u \neq o$ (og $v \neq o$), hvorfor også $\Lambda_{(v,u)} \in L \setminus \{N\}$.

Da

$\Lambda_{(u,v)} \cdot \Lambda_{(v,u)} = \Lambda_{(uv,vu)} = \Lambda_{(uv,uv)} = E$, er

$\Lambda_{(v,u)}$ inverst til $\Lambda_{(u,v)}$.

I alt er så $(L \setminus \{N\}, \cdot)$ en kommutativ gruppe.

Nu er <u>· distributiv med hensyn til +</u>.

$$(\Lambda_{(u_1,v_1)} + \Lambda_{(u_2,v_2)}) \cdot \Lambda_{(u_3,v_3)} = \Lambda_{(u_1v_2+v_1u_2,v_1v_2)} \cdot \Lambda_{(u_3,v_3)}$$
$$= \Lambda_{((u_1v_2+v_1u_2)u_3,v_1v_2v_3)}$$
$$= \Lambda_{(u_1v_2u_3+v_1u_2u_3,v_1v_2v_3)}$$

og

$$\Lambda_{(u_1,v_1)} \cdot \Lambda_{(u_3,v_3)} + \Lambda_{(u_2,v_2)} \cdot \Lambda_{(u_3,v_3)}$$
$$= \Lambda_{(u_1u_3,v_1v_3)} + \Lambda_{(u_2u_3,v_2v_3)} = \Lambda_{(u_1u_3v_2v_3+v_1v_3u_2u_3,v_1v_3v_2v_3)}$$
$$= \Lambda_{(u_1u_3v_2+u_2u_3v_1,v_1v_2v_3)} \cdot \Lambda_{(v_3,v_3)}$$
$$= \Lambda_{(u_1u_3v_2+u_2u_3v_1,v_1v_2v_3)}.$$

De fundne egenskaber ved + og · udtrykker, at <u>(L,+,·) er et kommutativt legeme</u>.

Vi vender os nu til sætningens punkt i):

Opgaven er at skaffe en delmængde M af L, der kan repræsentere de hele tal. Idet det hele tal q kan repræsenteres af "brøken $\frac{q}{1}$" er det nærliggende, at lade $\Lambda_{(q,1)}$ svare til q. Vi definerer derfor nu

(5) $M = \{\Lambda_{(q,1)} \mid q \in \mathbb{Z}\}$.

Vi har nu, at $(u,v) \in \Lambda_{(q,1)}$ hvis og kun hvis $(u,v) \sim (q,1)$, dvs. hvis og kun hvis $u = qv$. Altså er

$$\Lambda_{(q,1)} = \{(qv,v) \mid v \in \mathbb{Z} \setminus \{o\}\}.$$

Sætter vi for $q \in \mathbb{Z}$

(6) $\varphi(q) = \Lambda_{(q,1)}$

Lad være med at blive forskrækket over notationen med † og * osv. Den er desværre nødvendig på dette sted for at forhindre fejlslutninger. Men tænk på L" som $\{u \cdot v^{-1} \mid u \in Z,\ v \in Z \setminus \{o\}\}$, hvor kompositionen m.v. hidrører fra L'. Betegnelsen -1(L') skal angive invers i forhold til * i L'.

fås en definition på en afbildning φ: $Z \sim M$.

Denne afbildning <u>φ er en isomorfi</u>,

thi, at <u>φ er en homomorfi</u> følger af at der dels gælder, at

$\varphi(q_1+q_2) = \Lambda_{(q_1+q_2,1)}$

og

$\varphi(q_1) + \varphi(q_2) = \Lambda_{(q_1,1)} + \Lambda_{(q_2,1)} = \Lambda_{(q_1+q_2,1)} = \varphi(q_1+q_2)$,

og dels at

$\varphi(q_1q_2) = \Lambda_{(q_1q_2,1)} = \Lambda_{(q_1,1)} \cdot \Lambda_{(q_2,1)} = \varphi(q_1) \cdot \varphi(q_2)$.

Desuden er <u>φ injektiv</u>, fordi man af $\varphi(q_1) = \varphi(q_2)$ (dvs. $\Lambda_{(q_1,1)} = \Lambda_{(q_2,1)}$) kan slutte, at $(q_1,1) \sim (q_2,1)$, altså at $q_1 = q_2$.

Endelig er <u>φ surjektiv</u>, thi hvis $\Lambda \in M$ findes et $q \in Z$ og et $v \in Z \setminus \{o\}$, så at

$\Lambda = \Lambda_{(q,1)} = \varphi(q)$.

Alt i alt er φ en isomorfi mellem $(Z,+,\cdot)$ og $(M,+,\cdot)$.

Eftersom $(Z,+,\cdot)$ er en kommutativ integritetsring med ételement, er $(M,+,\cdot)$ det også. Da $\varphi(1) = \Lambda_{(1,1)} = E$, er ételementet i $(M,+,\cdot)$ det samme som ételementet i $(L,+,\cdot)$

Hermed er <u>i) vist</u>.

For at vise ii) skal vi betragte et vilkårligt Λ i L. Det har formen $\Lambda = \Lambda_{(u,v)}$ for et $u \in Z$ og et $v \in Z \setminus \{o\}$. Idet

$$\Lambda = \Lambda_{(u,v)} = \Lambda_{(u,1)} \cdot \Lambda_{(1,v)} = \Lambda_{(u,1)} \cdot \Lambda_{(v,1)}^{-1},$$

hvor $\Lambda_{(u,1)}$ og $\Lambda_{(v,1)} \in M$, er <u>ii) vist</u>.

Vi identificerer herefter $(Z,+,\cdot)$ med $(M,+,\cdot)$ og taler om $(Z,+,\cdot)$ som en <u>delring</u> af $(L,+,\cdot)$.

Vi skal nu vise iii), at hvis $(L',\dagger,*)$ er et kommutativt legeme der har $(Z,+,\cdot)$ som delring (i den ovenfor nævnte forstand), findes et dellegeme af $(L',\dagger,*)$ som er isomorft med $(L,+,\cdot)$.

Lad altså $(L',\dagger,*)$ være et kommutativt legeme, der omfatter $(Z,+,\cdot)$.

Benævnelsen $\cdot_Z$ og siden $+_Z$ refererer selvfølgelig til kompositionerne i Z. De indføres for at støtte dette korte øjeblik for at støtte at tungen holdes lige i munden.

Sættes

$$L'' = \{u * v^{-1(L')} \mid u \in Z,\ v \in Z \setminus \{o\}\},$$

er L" stabil over for $\dagger$,

idet det for $u_1, u_2 \in Z$, $v_1, v_2 \in Z \setminus \{o\}$ gælder, at

$$(u_1 * v_1^{-1(L')}) \dagger (u_2 * v_2^{-1(L')}) = (u_1 * v_2 \dagger v_1 * u_2) * (v_1 * v_2)^{-1(L')}$$

tilhører L", da $v_1 * v_2 \in Z \setminus \{o\}$.

At L" også er stabil over for * ses af,

at der for $u_1, u_2 \in Z$, $v_1, v_2 \in Z \setminus \{o\}$ gælder:

$$(u_1 * v_1^{-1(L')}) * (u_2 * v_2^{-1(L')}) = (u_1 * u_2) * (v_1 * v_2)^{-1(L')},$$

der tilhører L", fordi $v_1, v_2 \in Z \setminus \{o\}$.

Lad nu $\ell \in L$. Så findes i følge ii) et $u \in Z$ og et $v \in Z \setminus \{o\}$, så at

$$\ell = u \cdot v^{-1(L)}.$$

Sættes

$$(7)\quad \psi(\ell) = u * v^{-1(L')} \quad (\in L''),\quad v^{-1(L')} \neq o,$$

defineres en afbildning fra L til L". For at indse, at dette virkelig er tilfældet, skal vi godtgøre, at hvis $u' \in Z$ og $v' \in Z \setminus \{o\}$, og

$$(8)\quad u \cdot v^{-1(L)} = u' \cdot (v')^{-1(L)},$$

er også

$$(9)\quad u * v^{-1(L')} = u' * (v')^{-1(L')}.$$

Da L er et kommutativt legeme, er (8) ensbetydende med, at $u \cdot v' = u' \cdot v$.

Nu er alle u,v,u',v' elementer i Z. Idet (Z,+,·) er en delring af (L,+,·) er

(lo) $u \cdot_Z v' = u \cdot v' = u' \cdot v = u' \cdot_Z v$.

Da (Z,+,·) også var antaget at være en delring af (L',†,·) er (idet (lo) anvendes)

$u * v' = u \cdot_Z v' = u' \cdot_Z v = u' * v$,

altså

$u * v' = u' * v$.

Men det er netop, da $v, v' \in Z \setminus \{o\}$, ensbetydende med (9), hvorfor (7) fremstiller en definition af afbildningen ψ.

Afbildningen ψ er en isomorfi.

At ψ er en homomorfi følger af

$$\psi(\ell_1+\ell_2) = \psi(u_1\cdot v_1^{-1(L)} + u_2\cdot v_2^{-1(L)})$$
$$=\psi[(u_1\cdot v_2 + u_2\cdot v_1)\cdot(v_1\cdot v_2)^{-1(L)}] = (u_1\cdot v_2 + u_2\cdot v_1)*(v_1\cdot v_2)^{-1(L')}$$
$$= (u_1\cdot z^{v}_2 + u_2\cdot z^{v}_1)*(v_1\cdot v_2)^{-1(L')},$$

da $u_1, v_2, u_2, v_1 \in Z$.

Det sidste udtryk er videre lig med

$$(u_1*v_2 + u_2*v_1)*(v_1*v_2)^{-1(L')} = u_1*v_1^{-1} + u_2*v_2^{-1}$$
$$= \psi(\ell_1) + \psi(\ell_2).$$

Altså er $\psi(\ell_1+\ell_2) = \psi(\ell_1) + \psi(\ell_2)$.

Hvad den resterende homomorfiegenskab angår er

$$\psi(\ell_1\cdot\ell_2) = \psi(u_1\cdot v_1^{-1(L)})\cdot(u_2\cdot v_2^{-1(L)})$$
$$= \psi[(u_1\cdot u_2)\cdot(v_1\cdot v_2)^{-1(L)}] = (u_1\cdot u_2)*(v_1\cdot v_2)^{-1(L')}$$
$$= (u_1\cdot z u_2)*(v_1\cdot z v_2)^{-1(L')} = (u_1*u_2)*(v_1*v_2)^{-1(L')}$$
$$= (u_1*v_1^{-1(L')})*(u_2*v_2^{-1(L')})$$
$$= \psi(\ell_1) * \psi(\ell_2),$$

idet det fjerde og femte lighedstegn følger af, at u_1, u_2 og v_1, v_2 tilhører Z.

Således er ψ en homomorfi.

At ψ er surjektiv følger af, at det typiske element $u*v^{-1(L')}$ i L", med $u \in Z$ og $v \in Z \setminus \{o\}$, er lig med $\psi(u\cdot v^{-1(L)})$.

At endelig ψ er injektiv indses således:

Hvis $\psi(\ell_1) = \psi(\ell_2)$, dvs. hvis

$$u_1*v_1^{-1(L')} = u_2*v_2^{-1(L')}$$

for $u_1, u_2 \in Z$ og $v_1, v_2 \in Z \setminus \{o\}$, er $u_1*v_2 = u_2*v_1$, og dermed

$$u_1\cdot v_2 = u_1\cdot z v_2 = u_1*v_2 = u_2*v_1 = u_2\cdot z v_1 = u_2\cdot v_1,$$

hvilket viser, at

$$u_1\cdot v_2 = u_2\cdot v_1.$$

Men så er også $\ell_1 = u_1\cdot v_1^{-1(L)} = u_2\cdot v_2^{-1(L)} = \ell_2$

Hermed er iii) vist.

Måske er opfattelsen, at $\frac{u}{v} > o$ netop hvis u og v har samme fortegn endnu mere dagligdags. Det er imidlertid ubekvemt at benytte dette forhold direkte, idet det giver anledning til betragtning af to forskellige tilfælde, og dermed mere bogholderi.

Beviset for iv) er herefter gratis:

Lad $(L_1,+,\cdot)$ opfylde i) og ii). I følge iii) (herunder beviset for punktet) findes så et dellegeme $(L",+,\cdot)$ af $(L_1,+,\cdot)$, så at

$$L" = \{u \cdot_{L_1} v^{-1(L_1)} \mid u \in Z,\ v \in Z \setminus \{o\}\},$$

og så at $(L",+,\cdot)$ er isomorf med $(L,+,\cdot)$.

Eftersom $(L_1,+,\cdot)$ opfylder ii), er

$$L_1 = \{u \cdot_{L_1} v^{-1(L_1)} \mid u \in Z,\ v \in Z \setminus \{o\}\},$$

hvilket viser, at $L_1 = L"$. Men så er $(L_1,+,\cdot)$ isomorf med $(L,+,\cdot)$.

Hermed er sætningen bevist.

Det kommutative legeme, der i Sætning III.1 benæves $(L,+,\cdot)$ kaldes de rationale tals legeme og vil i fremtiden blive benævnt $(Q,+,\cdot)$. Nulelementet i Q betegnes o, ëtelementet 1. Disse elementer er, idet vi i kraft af i) i sætningen taler om $(Z,+,\cdot)$ som en delring af $(Q,+,\cdot)$, identiske med henholdsvis nul- og ëtelementet i Z. I stedet for $\wedge_{(u,v)}$ med v = o skriver vi (jfr. ii)) $\frac{u}{v}$. En undtagelse herfra gøres dog for klarhedens skyld i det næste afsnit.

Organiseringen af mængden af rationale tal som et ordnet legeme

Vi vil slutte behandlingen af de rationale tal med at overføre ordningsrelationen fra de hele tal til de rationale tal. Vi ønsker at etablere en ordning på $(Q,+,\cdot)$, som udvider ordningen på $(Z,+,\cdot)$, og som harmonerer med kompositionerne. I konstruktionen heraf går vi frem på følgende måde.

For et rationalt tal $r = \frac{u}{v}$, $u \in Z$, $v \in Z \setminus \{o\}$, gælder inden for den dagligdags opfattelse af de rationale tal, at $r > o$ hvis og kun hvis $uv > o$. Vi vil udnytte denne observation til en formel definition. Først må vi dog være sikre på, at enten har alle repræsentanter $\frac{u}{v}$ for r egenskaben $uv > o$, eller også har ingen den. Ellers kunne vi ikke opfatte denne egenskab ved repræsentanterne som en egenskab ved hele klassen r.

Den fornødne sikkerhed etableres i det formelle system på følgende måde:

Lad $r \in Q$, $r = \frac{u}{v}$ for et $u \in Z$ og et $v \in Z \setminus \{o\}$, så at $uv > o$ ($> $ forstået som $>_Z$). Hvis endvidere $\frac{u}{v} = r$ for et $u_1 \in Z$ og et $v_1 \in Z \setminus \{o\}$ vil også $u_1 v_1 > o$. Da nemlig

$$\frac{u}{v} = \frac{u_1}{v_1},$$

vil $uv_1 = vu_1$, og dermed

$$(uv_1)^2 = uv_1 uv_1 = (uv)(v_1 u_1).$$

Idet det for ethvert $a \in Z$ gælder, at $a^2 > o$, hvis $a \neq o$, vil $(uv_1)^2 > o$. (At $a^2 > o$, hvis $a \neq o$, skyldes, at enten er $a > o$ eller $a < o$ (trichotymien af den irrefleksive ordning i Z). Er $a > o$ er $a^2 = a \cdot a > a \cdot o = o$. Hvis $a < o$ er $-a > o$ og dermed $-a^2 = a(-a) < o \cdot (-a) = o$, hvoraf $a^2 > o$.)

Da $u \neq o$ (fordi $uv > o$) og $v_1 \neq o$, er $uv_1 \neq o$, og dermed

$$(uv)(v_1 u_1) = (uv_1)^2 > o.$$

Nu må, da $uv > o$, $v_1 u_1 > o$. Var nemlig alternativt $v_1 u_1 \leq o$ måtte $(uv)(v_1 u_1) \leq o$, hvilket ikke er tilfældet. Dermed er påstanden bevist.

Vi definerer nu

$$(11) \quad Q_+ = \{\Lambda_{(u,v)} \mid uv > o\} .$$

De umiddelbart foregående overvejelser sikrer, at hvis (u_1, v_1) ligger i $\Lambda_{(u,v)}$ med $uv > o$ er $u_1 v_1 > o$.

Sætter vi videre

$$(12) \quad Q_- = \{\Lambda_{(u,v)} \mid uv < o\},$$

ses ud fra det foregående, at $Q_+ \cup Q_- = \emptyset$.

Hvis $uv = o$ ($v \in Z \setminus \{o\}$) er $u = o$. Men så er $\Lambda_{(u,v)} = N$. Det ses, at $N \notin Q_+ \cup Q_-$. For et vilkårligt $\Lambda_{(u,v)}$ gælder således <u>enten</u> at $\Lambda_{(u,v)} = N$, <u>eller</u> at $\Lambda_{(u,v)} \in Q_+$ (nemlig hvis $uv > o$) samtidig med, at $-\Lambda_{(u,v)} = \Lambda_{(-u,v)} \in Q_-$ ($-uv < o$), <u>eller</u> at $\Lambda_{(u,v)} \in Q_-$ (hvis $uv < o$) samtidig med, at $-\Lambda_{(u,v)} = \Lambda_{(-u,v)} \in Q_+$ ($-uv > o$). Ingen af delene kan indtræffe samtidig. Derfor udgør Q_+, $\{o\}$, Q_- en klassedeling af Q:

$$\underline{(13) \quad Q = Q_- \cup \{o\} \cup Q_+}$$

Formuleret i ord: Summer og produkter af positive rationale tal er positive.

Læg mærke til, at definitionen respekterer vores "dagligdags" fornemmelse vedrørende ordningen på de rationale tal.

Elementerne i Q_+ kaldes de positive rationale tal, elementerne i Q_- de negative rationale tal. Nedenfor vil denne sprogbrugs overensstemmelse med den ordningsrelation der indføres blive påvist.

I det følgende har vi brug for et par egenskaber ved Q_+ som det er bekvemt at have formuleret på forhånd:

Hvis $q = \frac{u_1}{v_1} \in Q_+$ og $r = \frac{u_2}{v_2} \in Q_+$ ($v_1 \neq o$, $v_2 \neq o$), vil $q+r = (u_1v_2+v_1u_2)/v_1v_2 \in Q_+$ og $qr = (u_1u_2)/v_1v_2 \in Q_+$.

Thi for det første er
$(u_1v_2+v_1u_2)v_1v_2 = uv_1v_2^2+u_2v_2v_1^2 > o$, da $u_1v_1 > o$,
og dermed $u_1v_1^2 > o \cdot v_2^2 = o$, og $u_2v_2 > o$ og dermed $u_2v_2v_1^2 > o$.
Og for det andet er
$(u_1u_2)(v_1v_2) = (u_1v_1)(u_2v_2) > o$,
da $u_1v_1 > o$ og $u_2v_2 > o$.

Definition: Vi definerer en relation $>_Q$ i Q ved

(14) $\quad r >_Q q \Leftrightarrow (r-q) \in Q_+$.

Der gælder så

Sætning III.2. Relationen $>_Q$ er en irrefleksiv ordningsrelation med trichotymi i Q. Den harmonerer med + og ·, dvs. opfylder for givne $r, q \in Q$:

(15) $\forall s \in Q: r >_Q q \Leftrightarrow r+s >_Q q+s$
(16) $\forall s \in Q\ (s >_Q o): r >_Q q \Leftrightarrow rs >_Q qs$.

Endvidere er $>_Q$ en udvidelse af $>$ (på Z), idet

(17) $\forall q,r \in Z: r >_Q q \Leftrightarrow r > q$.

Et legeme med en sådan ordningsrelation (excl. (17)) kaldes et ordnet legeme. Sætningen viser altså, at $(Q,+,\cdot,<_Q)$ er et ordnet legeme.

Bevis:

Trichotymien er oplagt,

thi for vilkårlige q,r (i Q) er (i kraft af (13)) enten $r-q = o$ eller $r-q \in Q_+$ eller $q-r \in Q_+$, men ikke to af mulighederne samtidig. Dette svarer i kraft af definitionen

((14)) til at enten er $r = q$ eller $q >_Q r$ eller $r >_Q q$, og disse muligheder er gensidigt udelukkende.

At $>_Q$ er irrefleksiv er oplagt, da for ethvert $r \in Q$, $r \not>_Q r$ ($o \notin Q_+$).

Asymmetrien fremgår af trichotymien. Hvis nemlig $r >_Q q$, kan der ikke samtidig gælde, at $q >_Q r$.

Hvad endelig transitiviteten angår, følger den således:

Hvis $s >_Q r$ og $r >_Q q$, vil $s-r \in Q_+$ og $r-q \in Q_+$. I kraft af bemærkningerne før definitionen side 114 vil så $s-q = (s-r)+(r-q) \in Q_+$, hvorved $s >_Q q$.

Harmoniegenskaben (15) er en umiddelbar konsekvens af, at for ethvert $s \in Q$ er $r-q \in Q_+$ ensbetydende med, at $(r+s)-(q+s) = r-q \in Q_+$.

For at bevise (16)

skal vi betragte et givet s, $s >_Q o$ (dvs. $s \in Q_+$). Hvis nu $r-q \in Q_+$ vil $rs-qs = (r-q)s \in Q_+$, jfr. bemærkningerne side 114. Altså vil - hvis $r >_Q q$ - $rs >_Q qs$. Er omvendt $rs >_Q qs$, må $r >_Q q$. Ellers var nemlig $r = q$, eller $r <_Q q$, hvorved $rs = qs$ eller $rs <_Q qs$ (på grund af det netop beviste), i strid med trichotymien.

Sætningen er bevist, når vi har indset, at $>_Q$ er en udvidelse af $>$ ($>_Z$). Lad $q,r \in Z$. Vi har så (da $r-q \in Z$):

$r >_Q q \Leftrightarrow r-q \in Q_+ \Leftrightarrow \frac{r-q}{1} \in Q_+$, hvilket i kraft af definitionen af Q_+ ((11)) er ensbetydende med, at $(r-q)\cdot 1 >_Z o$, dvs. med at $r-q >_Z o$, der på sin side er ækvivalent med, at $r >_Z q$. Dermed er det ønskede bevist.

Q.E.D.

Den til $>_Q$ svarende <u>refleksive ordningsrelation</u> $\geq_Q$ defineres således:

<u>Definition</u>: $r \geq_Q q \Leftrightarrow r >_Q q \vee r = q$.

Der gælder nu:

<u>Sætning. III.3</u>. For vilkårlige $r,q \in Q$ gælder

(18) $\forall s \in Q$: $r \geq_Q q \Leftrightarrow r+s \geq_Q q+s$

Obs! Vi er i (19) nødt til at kræve $s >_Q o$ og ikke bare $s \geq_Q o$. Hvis $s = o$ gælder implikationen "$\Leftarrow$" ikke.

Der benyttes to gange, at når $q < s$, er $q/2 < s/2$. Dette er en anvendelse af harmoniegenskaben (16). Bemærk også, at harmoniegenskaben (15) er i spil.

Læg mærke til at denne definition kan fremsættes i ethvert ordnet legeme $(L,+,\cdot,<)$ - det skal vi bruge senere.

(19) $\forall s \in Q\ (s >_Q o)$: $r \geq_Q q \Leftrightarrow rs \geq_Q qs$

(20) $r \geq_Q q \Leftrightarrow r \geq_Z q$, for r,q i Z

Bevis:

Der er tale om en serie simple efterprøvninger.

Ad (18): Vi har for ethvert s, at

$r \geq_Q q \Leftrightarrow r = q \vee r >_Q q \Leftrightarrow r = q \vee r+s >_Q q+s \Leftrightarrow r+s = q+s$
$\vee r+s >_Q q+s \Leftrightarrow r+s \geq_Q q+s$.

Ad (19): For $s >_Q o$ har vi, at $r \geq_Q q \Leftrightarrow r = q \vee r >_Q q \Leftrightarrow r = q$
$\vee rs >_Q qs \Leftrightarrow rs = qs \vee rs >_Q qs \Leftrightarrow rs \geq_Q qs$.

Både for (18) og (19) følger de to yderste biimplikationer af definitionen på $\geq_Q$, mens den anden følger af (15) og den tredje af forkortningsreglerne for henholdsvis addition og multiplikation i Z.

Ad (20): $r \geq_Q q \Leftrightarrow r = q \vee r >_Q q \Leftrightarrow r = q \vee r >_Z q \Leftrightarrow r \geq_Z q$.

Q.E.D.

Der er efter disse sætninger ingen grund til længere at opretholde tegnet $>_Q$ ($\geq_Q$) til adskillelse fra $>$ ($\geq$). Vi skal derfor fremover kun bruge de sidstnævnte tegn for ordningerne på Q.

Sætning III.4. De rationale tals legeme er tæt ordnet ved $<$, dvs. for ethvert par $q,s \in Q$, hvor $q < s$, findes et $r \in Q$, så at $q < r < s$.

Bevis: Sættes $r = \frac{q+s}{2}$ er $q = \frac{q}{2} + \frac{q}{2} < \frac{q}{2} + \frac{s}{2} < \frac{s}{2} + \frac{s}{2} = s$, hvilket beviser det ønskede.

I $(Q,+,\cdot,<)$ kan der - som i ethvert ordnet legeme - indføres en numerisk værdi.

Definition: Ved den numeriske værdi af det rationale tal r forstås tallet

(21) $|r| = \max\{r,-r\}$.

Egenskaberne ved den numeriske værdi samles i

For dem som har lært lineær algebra vil det fremgå, at den numeriske værdi er en norm, hvis man opfatter de rationale tal som et vektorrum over sig selv som legeme. Hvilke af egenskaberne (22)-(3o) godtgør, at den numeriske værdi er en norm?

Kontrollér alle påstande undervejs i beviset og henfør dem til resultater, der er etableret i det foregående.

Sætning III.5. For vilkårlige q,r i Q gælder:

(22) $|r| = \begin{cases} r, & \text{hvis } r \geq o \\ -r, & \text{hvis } r \leq o \end{cases}$

(23) $|r| \geq o$, og lighedstegnet gælder netop hvis $r = o$

(24) $|-r| = |r|$

(25) $||r|| = |r|$

(26) $-|r| \leq r \leq |r|, -|r| \leq -r \leq |r|$

(27) $|r+q| \leq |r|+|q|$ (trekantsuligheden)

(28) $||r|-|q|| \leq |r-q|$

(29) $|rq| = |r||q|$

(3o) $|r^{-1}| = |r|^{-1}$.

Bevis:

Ni simple checks:

Ad (22): Hvis $r \geq o$, er $r \geq o \geq -r$ og dermed $|r| = \max\{r,-r\} = r$. Hvis $r \leq o$, er $-r \geq o \geq r$, og dermed $|r| = \max\{r,-r\} = -r$.

Ad (23): Hvis $r \geq o$ er $|r| = r \geq o$. Hvis $r \leq o$, er $|r| = -r \geq o$. Hvis $r = o$ er $-r = o$ og $|r| = o$. Hvis $|r| = o$ er $r = o$ eller $-r = o$. Så er $r = o$.

Ad (24): $|-r| = \max\{-r,-(-r)\} = \max\{r,-r\} = |r|$.

Ad (25): $||r|| = \max\{|r|, -|r|\} = \max\{r,-r\} = |r|$.

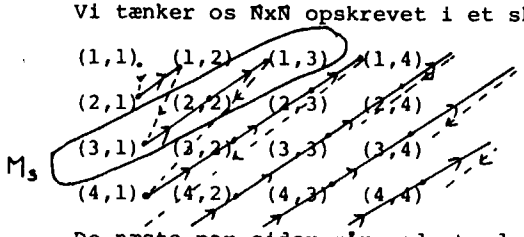
Ad (26): Af definitionen på numerisk værdi følger, at $r \leq |r|$ og $-r \leq |r|$ og dermed, at $-|r| \leq -r$ og $r \geq -|r|$.

Ad (27): Af (26) følger, at $r+q \leq |r|+|q|$ og $-r-q \leq |r|+|q|$, hvoraf $|r+q| = \max\{r+q,-r-q\} \leq |r|+|q|$.

Ad (28): Af $|r| = |r-q+q| \leq |r-q|+|q|$ følger, at $|r|-|q| \leq |r-q|$. Tilsvarende fås, at $|q| \leq |q-r|+|r| = |r-q|+|r|$, og at $-(|r|-|q|) = |q|-|r| \leq |r-q|$. Så er $||r|-|q|| = \max\{|r|-|q|, -(|r|-|q|)\} \leq |r-q|$.

Ad (29): Hvis $q \geq o$ og $r \geq o$, er $rq \geq o$, og dermed $|rq| = rq = |r||q|$. Hvis $q \leq o$ og $r \leq o$ er $-q \geq o$ og $-r \geq o$ og dermed $|rq| = |(-r)(-q)| = |-r||-q| = (-r)(-q) = |r||q|$. Hvis $q \leq o$ og $r \geq o$ er $|rq| = |-rq| = |r(-q)| = |r||-q| = |r||q|$. Tilsvarende for $r \leq o$ og $q \geq o$.

Ad (3o): Denne egenskab følger af, at $1 = |rr^{-1}| = |r||r^{-1}|$, for $r \neq o$. Q.E.D.



Vi tænker os $\mathbb{N}x\mathbb{N}$ opskrevet i et skema: At godtgøre numerabiliteten af mængden $\mathbb{N}x\mathbb{N}$ kommer ud på at opstille dens elementer i en rækkefølge. I den skitserede samles parrene i mængder, M_p, efter deres sum. Derefter "grovnummereres" efter summen og "finnummereres" inden for M_p efter stigende første-koordinat.

De næste par sider går med at udmønte denne idé inden for den her opstillede ramme.

Til brug for senere formål viser vi

Sætning III.6. For ethvert rationalt tal r findes et naturligt tal n, så at $r < n$.
(Et ordnet legeme indeholdende et eksemplar af de naturlige tal, som besidder denne egenskab, kaldes arkimedisk ordnet.)

Bevis:
Hvis $r \leq o$ er $n = 1 > r$. Vi antager derfor, at $r > o$, og at $r = \frac{u}{v}$ for et par u,v i $\mathbb{N}$ ($v \neq o$). Nu findes et $n \in \mathbb{N}$, så at $nv > u$. Hvis nemlig $v = 1$, vil $n = 2u$ opfylde, at $nv = 2u > u$. Thi da $2 > 1$ og $u > o$ vil ((16)) $2u > u$. Er i stedet $v > 1$, vil $uv > u$, således at vi med $n = u$ har $nv > u$.

Hermed er sætningen bevist, idet vi af $nu > u$ slutter ((16)), at $n = \frac{nv}{v} > \frac{u}{v} = r$.

*

Behandlingen af de rationalt tal afsluttes med en omtale af ækvipotensforhold. Hovedresultatet er, at mængden af rationale tal er ækvipotent med $\mathbb{N}$. Inden vi beviser det vil vi anføre og bevise et hjælperesultat, der imidlertid også har en vis interesse i sig selv :

Mængden $\mathbb{N}x\mathbb{N}$ er ækvipotent med $\mathbb{N}$.

Fra et intuitivt synspunkt er det nemt at overbevise sig om denne påstand, jfr. kommentarerne på siden overfor. Skal denne intuition omsættes til et præcist bevist er der imidlertid mange detaljer at holde rede på. De har en tendens til at sløre billedet, men kan f.eks. se således ud:

Lad os for alle $p \in \mathbb{N}$ betragte mængderne

$$M_p = \{(m,n) \in \mathbb{N}x\mathbb{N} \mid m+n = p+1\}$$

(dvs. $M_1 = \{(1,1)\}$, $M_2 = \{(1,2),(2,1)\}$, $M_3 = \{(1,3),(2,2),(3,1)\}$ osv.). Det ses, at $M_p = \{(1,p),(2,p-1),\ldots,(p-1,2),(p,1)\}$, og at antallet af elementer i M_p er p.

Mængderne M_p frembringer øjensynlig en klassedeling af $\mathbb{N}x\mathbb{N}$, idet det vilkårlige par $(m,n) \in \mathbb{N}x\mathbb{N}$ tilhører netop én af dem. Det sam-

Tallet $\chi(m,n)$ er det nummer parret (m,n) får tildelt i den valgte rækkefølge i $\mathbb{N}x\mathbb{N}$. Tallet består af to led, dels $\frac{1}{2}(p-1)p$, der angiver "grovnummeret", dvs. det samlede antal elementer i de M-mængder der går forud for den, M_p, som (m,n) ligger i, dels m, der angiver "finnummeret", dvs. p^{te} elementets plads inden for M_p. Summen af de to led angiver så den samlede plads i rækkefølgen.

Hemmeligheden med denne opspaltning af $\mathbb{N}$ er at tallene i den p'te klasse netop er numrene på de $\mathbb{N}x\mathbb{N}$-elementer, der hører hjemme i M_p. Denne opdeling har vi brug for, når vi om lidt skal godtgøre, at χ er bijektiv.

lede antal elementer i mængderne $M_1,\ldots,M_{p-1}$ $(p \geq 2)$, dvs. i mængden $M_1 \cup \ldots \cup M_{p-1}$, er $1+2+\ldots+(p-2)+(p-1) = \frac{1}{2}(p-1)p$.

Vi vil nu fremskaffe en bijektiv afbildning af $\mathbb{N}x\mathbb{N}$ på $\mathbb{N}$. Det sker således:

For $(m,n) \in \mathbb{N}x\mathbb{N}$ er $p = (m+n-1)$ det entydigt bestemte naturlige tal, for hvilket $(m,n) \in M_p$: derefter sættes

$$\chi(m,n) = \tfrac{1}{2}(p-1)p + m = \tfrac{1}{2}(m+n-2)(m+n-1) + m.$$

Det ses, at $(m,n) \in \mathbb{N}$, idet enten $m+n-2$ eller $m+n-1$ er lige, hvorved $\frac{1}{2}(m+n-2)(m+n-1)$ er et naturligt tal eller o. Derved er χ en afbildning fra $\mathbb{N}x\mathbb{N}$ ind i $\mathbb{N}$,

$$\chi: \mathbb{N}x\mathbb{N} \sim \mathbb{N}.$$

Vi skal vise, at χ er bijektiv. Til den ende har vi brug for nogle hjælpebetragtninger.

"Intervallerne" $I_p = \{\frac{1}{2}(p-1)p + 1,\ldots,\frac{1}{2}p(p+1)\} = \{q \in \mathbb{N} \mid \frac{1}{2}(p-1)p + 1 \leq q \leq \frac{1}{2}p(p+1)\}$), $p \geq 2$, udgør sammen med $\{1\}$ en klassedeling af $\mathbb{N}$:

$$\mathbb{N} = \{1\} \cup \{2,3\} \cup \{4,5,6\} \cup \ldots$$
$$= \{1\} \cup \bigcup_{p\geq 2} \{\tfrac{1}{2}(p-1)p + 1,\ldots,\tfrac{1}{2}p(p+1)\}.$$

Thi:

Lad $p,p' \geq 2$ og $p \neq p'$, hvor vi kan antage, at $p' > p \geq 2$. Så er først I_p og $I_{p'}$ disjunkte. For hvis $q \in I_p$ og $q' \in I_{p'}$, er da $p \leq p'-1$ -

$$q \leq \tfrac{1}{2}p(p+1) < \tfrac{1}{2}p(p+1)+1 \leq \tfrac{1}{2}(p'-1)(p'-1+1)+1 = \tfrac{1}{2}(p'-1)p'+1 \leq q'$$

dvs. $q < q'$. Der kan derfor ikke være noget fælles element i de to intervaller. At de sammen med $\{1\}$ udgør hele $\mathbb{N}$ fremgår på denne måde:

Lad $q \in \mathbb{N}$. Er $q = 1$ vil $q \in \{1\}$. Vi antager derfor, at $q > 1$. Mængden $S = \{p \in \mathbb{N} \mid p \geq 2 \text{ og } \frac{1}{2}(p-1)p+1 \leq q\}$ er en opad begrænser delmængde af $\mathbb{N}$ (f.eks. begrænset af $2(q+1)$) og dermed af $\mathbb{Z}$. Den har derfor et største element, som vi benævner $p(q)$. Pr. definition gælder

$$\tfrac{1}{2}(p(q)-1)p(q) + 1 \leq q$$

Parret (m_o,n_o) fremkommer ved at der "regnes baglæns" i forhold til den på s. 123-124 nævnte opspaltning af $\mathbb{N}$. Det par (m_o,n_o), der skal have nummer q, må findes i den klasse $M_{p(q)}$, hvis "interval af numre" indeholder q. Så er (m_o,n_o) bestemt dels af kravet om at $m_o+n_o = p(q)+1$, hvoraf "grovnummeret" $\frac{1}{2}(p(q)-1)p(q)$ fremgår, dels af at m_o = finnummer = endeligt nummer+grovnummer = $q - \frac{1}{2}(p(q)-1)p(q)$, og endelig af, at $n_o = p(q)+1-m_o$.

Nu må desuden

$$q \leq \tfrac{1}{2}p(q)(p(q)+1).$$

Ellers ville jo $q > \frac{1}{2}p(q)(p(q)+1)$ og videre $q \geq \frac{1}{2}p(q)(p(q)+1) + 1$. Men det ville betyde, at $p(q)+1 \in S$, i strid med at $p(q)$ er det største element i S. Dette viser, at $q \in I_{p(q)}$ - og at q ikke tilhører nogen af de øvrige "intervaller".

Vi er nu parate til at vise at <u>χ er bijektiv</u>. Lad $q \in \mathbb{N}$. Hvis $q = 1$ er $q = 1 = \chi(1,1)$. Der gælder jo, at $(1,1) \in M_1$, så at $p(1,1) = 1$, hvorved $\chi(1,1) = \frac{1}{2}(1-1)\cdot 1+1 = 1$. Lad dernæst $q > 1$. I følge det ovenstående findes netop ét "interval", nemlig $I_{p(q)}$, som q tilhører. Nu betragtes parret

$$(m_o,n_o) = (q-\tfrac{1}{2}(p(q)-1)p(q),\ p(q)+1 - (q-\tfrac{1}{2}(p(q)-1)p(q))).$$

Det tilhører $\mathbb{N}\times\mathbb{N}$, for dels er $q-\frac{1}{2}(p(q)-1)p(q) \geq 1$ i kraft af definitionen på $p(q)$, dels er $p(q)+1 - q + \frac{1}{2}(p(q)-1)p(q) = 1-q + \frac{1}{2}p(q)(p(q)+1) \geq 1$, da $q \in I_{p(q)}$.

Desuden er åbenbart $m_o+n_o = p(q)+1$, så at $(m_o,n_o) \in M_{p(q)}$. Da $(m_o,n_o) \in M_{p(q)}$ er

$$\chi(m_o,n_o) = \tfrac{1}{2}(p(q)-1)p(q) + m_o = \tfrac{1}{2}(p(q)-1)p(q) + q - \tfrac{1}{2}(p(q)-1)p(q) = q.$$

Men det viser, at q er indfanget som billedet ved χ af et par, (m_o,n_o), i $\mathbb{N}\times\mathbb{N}$. Altså er χ <u>surjektiv</u>.

Tilbage står at indse, at χ er injektiv. Lad derfor (m,n) og (m',n') tilhøre $\mathbb{N}\times\mathbb{N}$. Vi antager, at $\chi(m,n) = \chi(m',n')$, dvs.

$$(31)\quad \tfrac{1}{2}(m+n-2)(m+n-1) + m = \tfrac{1}{2}(m'+n'-2)(m'+n'-1) + m'$$

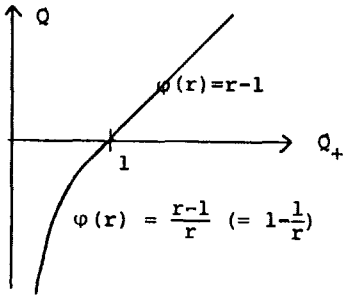
Der foreligger nu to muligheder. Enten ligger (m,n) og (m',n') i den samme M_p-klasse., eller i hver sin. Ligger de i den samme klasse, er $m+n-1 = m'+n'-1$. Så sluttes straks, af (31), at $m = m'$, og videre, at $n' = n$.
Altså er $(m,n) = (m',n')$. Ligger derimod (m,n) og (m',n') i hver sin klasse, er $m+n-1 \neq m'+n'-1$, lad os sige $m+n-1$ mindst. Vi får så

$$\chi(m,n) = \tfrac{1}{2}(m+n-2)(m+n-1) + m \leq \tfrac{1}{2}(m+n-2)(m+n-1) + (m+n-1)$$

(idet $m \leq m+n-1$), og videre $= \frac{1}{2}(m+n)(m+n-1)$
$< \frac{1}{2}(m'+n'-1)(m'+n'-2)$ (fordi $m+n \leq m'+n'-1$)

Også andre, analoge, veje er naturligvis til rådighed. Vi kunne f.eks. først vise at $\mathbb{Q}$ er ækvipotent med en delmængde af $\mathbb{Z}\times\mathbb{Z}$, derefter at $\mathbb{Z}\times\mathbb{Z}$ er ækvipotent med $\mathbb{N}$, således at $\mathbb{Q}$ er ækvipotent med en (uendelig) delmængde af $\mathbb{N}$ og dermed numerabel.

Kernen i dette skridt kan illustreres grafisk:



$< \frac{1}{2}(m'+n'-2)(m'+n'-1) + m' = \chi(m',n')$.

Dette viser, at $\chi(m,n) < \chi(m',n')$ i strid med forudsætningen. Men så kan (m,n) og (m',n') ikke ligge i hver sin klasse. Alt i alt er $(m,n) = (m',n')$. Derved er injektiviteten, og altså også bijektiviteten, bevist.

Vi vender os nu mod vort egentlige ærinde i denne sag.

Sætning III.7. Mængden $\mathbb{Q}$ af rationale tal er numerabel, dvs. ækvipotent med $\mathbb{N}$.

Bevis:
Vi viser først, at (a) $\mathbb{Q}$ er ækvipotent med mængden af positive rationale tal $\mathbb{Q}_+$, dernæst (b), at $\mathbb{Q}_+$ er ækvipotent med en delmængde af $\mathbb{N}\times\mathbb{N}$, og endelig (c), at denne delmængde er uendelig, og dermed ækvipotent med $\mathbb{N}$.

(a) Lad $r \in \mathbb{Q}_+$. Så sættes

$$\varphi(r) = \begin{cases} (r-1)/r & \text{for } 0 < r < 1 \\ r-1 & \text{for } r \geq 1. \end{cases}$$

Dette definerer φ som en afbildning fra $\mathbb{Q}_+$ til $\mathbb{Q}$,

$$\varphi: \mathbb{Q}_+ \sim \mathbb{Q}.$$

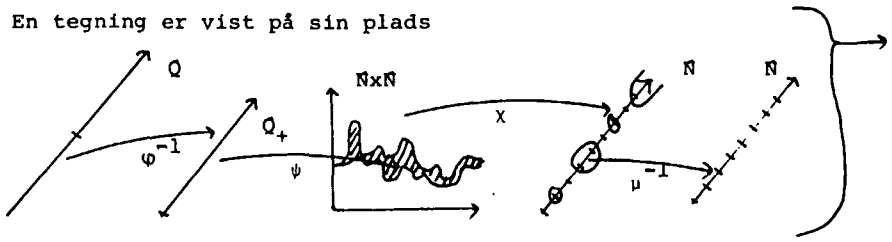
Vi vil vise, at φ er bijektiv. Først bemærkes, at hvis $0 < r < 1$, er $\varphi(r) < 0$ (idet $(r-1)/r < (1-1)/r = 0$), og at $\varphi(r) \geq 0$ for $r \geq 1$ $(r-1 \geq 0)$.

Injektiviteten af φ ses på denne måde: Lad $r,s \in \mathbb{Q}_+$, $r \neq s$. Hvis r og s ligger i hver sin af de to mængder $\{t \in \mathbb{Q} \mid 0 < t < 1\}$ og $\{t \in \mathbb{Q} \mid t \geq 1\}$ har $\varphi(r)$ og $\varphi(s)$ modsat fortegn (den ene værdi kan dog være 0). Ligger r og s begge i $\{t \in \mathbb{Q} \mid 0 < t < 1\}$ må $\varphi(r) = (r-1)/r$ og $\varphi(s) = (s-1)/s$. Nu må $\varphi(r) \neq \varphi(s)$. Var nemlig $\varphi(r) = \varphi(s)$ ville $rs-s = rs-r$, dvs. $-s = -r$, i strid med at $r \neq s$. Den sidste mulighed er at r og s begge ligger i $\{t \in \mathbb{Q} \mid t \geq 1\}$. Derved er $\varphi(r) = r-1$ og $\varphi(s) = s-1$. Det er da oplagt, at $\varphi(r) \neq \varphi(s)$; ellers var jo $r-1 = s-1$, i strid med at $r \neq s$. Under alle de behandlede omstændigheder bliver altså $\varphi(r) \neq \varphi(s)$, hvilket viser injektiviteten af φ.

Surjektiviteten af φ følger af: Lad $t \in \mathbb{Q}$. Hvis $t \geq 0$ vil $r = t+1 \geq 1$, og dermed $t = r-1 = \varphi(r)$. Hvis $t < 0$ er $1 < 1-t$ og dermed

Idéen i (b) er et repræsentere et positivt rationalt tal r med et entydigt bestemt par af naturlige tal fra den klasse af par som r jo er. Og det par der vælges er det med den laveste nævner. (At det findes kræver selvsagt et bevis.) Denne repræsentation anskues så som en afbildning $\varphi: Q_+ \rightsquigarrow \mathbb{N}\times\mathbb{N}$ - og resten er efterprøvninger.

En tegning er vist på sin plads



$o < 1/(1-t) < 1$. Sættes $r = 1/(1-t)$ er $r \in Q_+$ og

$$\varphi(r) = \frac{r-1}{r} = \frac{1/(1-t) - 1}{1/(1-t)} = t.$$

I alle tilfælde er $t \in Q$ indfanget som billede ved φ af et element i Q_+. Det beviser, at φ er surjektiv.

(b) Lad igen $r \in Q_+$. Så har r formen $r = \Lambda_{(p,q)}$ for passende hele tal p og q. Det kan øjensynlig opnås, at både p og q tilhører $\mathbb{N}$. Nu er

$$\{v \in \mathbb{N} \mid \exists u \in \mathbb{N}: (u,v) \in \Lambda_{(p,q)}\}$$

en delmængde af $\mathbb{N}$, hvorfor den har et mindste element, v(r). Til det findes et $u(r) \in \mathbb{N}$, så at $(u(r),v(r)) \in \Lambda_{(p,q)}$. Dette u(r) er entydigt bestemt. Opfyldte nemlig u' at $(u',v(r)) \in \Lambda_{(p,q)}$, ville $(u',v(r)) \sim (u(r),v(r))$, dvs. $u'v(r) = u(r)v(r)$. Da v(r) ikke er o, må så $u' = u(r)$.

Ved $r \rightsquigarrow (u(r),v(r))$ defineres derfor en afbildning ψ af Q_+ ind i $\mathbb{N}\times\mathbb{N}$,

$$\psi: Q_+ \rightsquigarrow \mathbb{N}\times\mathbb{N}.$$

Denne afbildning er åbenbart injektiv. Vi har nemlig at $(u(r),v(r)) \in \Lambda_{(p,q)} = r$. Hvis derfor $r,s \in Q_+$, $r \neq s$, vil tilsvarende $(u(s),v(s)) \in s$. Men når $r \neq s$ er de $\sim$ som klasser betragtet - disjunkte , hvorfor $\psi(r) = (u(r),v(r)) \neq (u(s),v(s)) = \psi(s)$.

Når ψ er injektiv er Q_+ ækvipotent med $\psi(Q_+) \subseteq \mathbb{N}\times\mathbb{N}$.

(c) Mængden $\chi(\psi(Q_+))$ er (se bemærkningerne forud for Sætning III.7) en delmængde af $\mathbb{N}$. Kan vi vise, at denne delmængde er ækvipotent med $\mathbb{N}$, f.eks. gennem afbildningen μ^{-1}, er i alt Q ækvipotent med $\mathbb{N}$, nemlig gennem afbildningen (jfr. punkt (a) og (b))

$$\mu^{-1} \circ \chi \circ \psi \circ \varphi^{-1}.$$

At $\chi(\psi(Q_+))$ er ækvipotent med $\mathbb{N}$ vises gennem et lidt mere generelt resultat, nemlig at en delmængde af $\mathbb{N}$, der ikke er opad begrænset, er ækvipotent med $\mathbb{N}$. At mængden $\chi(\psi(Q_+))$ faktisk ikke er opad begrænset kan vi overbevise os om ved at betragte et vilkårligt $n \in \mathbb{N}$. Anskuet som element i Q_+ opfylder n, at $(u(n),v(n)) = (n,1)$. Med betegnelsen fra side 124 vil $(n,1) \in M_n$, hvorved

Pointen i beviset er at nummerere elementerne i M efter deres størrelse. Det gøres ved først at udpege det mindste element i M, derefter det mindste i restmængden osv., idet det hver gang udnyttes at disse minima eksisterer fordi $\mathbb{N}$ er velordnet. Når M ikke er opad begrænset ender denne proces ikke. Tilbage står så blot at give denne pointe formelt kød og blod.

$\chi(\psi(n)) = \frac{1}{2}(n-1)n + n > n$, når $n > 1$. Dette viser, at der findes vilkårligt store elementer i $\chi(\psi(n))$.

Vi mangler at vise, at en ikke opad begrænset delmængde M af $\mathbb{N}$ ($M \neq \emptyset$) er ækvipotent med $\mathbb{N}$. Eftersom $\mathbb{N}$ er velordnet har mængden M et mindste element, $\mu(1)$. Så er $M \setminus \{\mu(1)\}$ ikke tom. Ellers var jo $M = \{\mu(1)\}$, i strid med at M ikke har noget største element. Nu findes et mindste element, $\mu(2)$, i $M \setminus \{\mu(1)\}$. Øjensynlig må $\mu(1) < \mu(2)$, da de er indbyrdes forskellige elementer i M, hvori $\mu(1)$ er mindst. Alment: Vi definerer rekursivt for $n \in \mathbb{N}$

$$\mu(n+1) = \min (M \setminus \{\mu(1),\ldots,\mu(n)\}),$$

hvilket er muligt, da $M \setminus \{\mu(1),\ldots,\mu(n)\} \neq \emptyset$ fordi ellers ville $M = \{\mu(1),\ldots (n)\}$ i strid med at M ikke har noget største element. Der gælder $\mu(n) < \mu(n+1)$ for alle $n \in \mathbb{N}$. Thi for det første er $\mu(n) \neq \mu(n+1)$, da $\mu(n+1) \in M \setminus \{\mu(1),\ldots,\mu(n)\}$; for det andet vil $\mu(n+1) \in M \setminus \{\mu(1),\ldots\mu(n-1),\mu(n)\} \subseteq M \setminus \{\mu(1),\ldots,\mu(n-1)\}$. Imidlertid er jo $\mu(n)$ det mindste element i den sidstnævnte mængde, hvorfor $\mu(n) \leq \mu(n+1)$. Da de to elementer i følge det foregående ikke er identiske, er $\mu(n) < \mu(n+1)$. Det viser, at afbildningen $\mu: n \rightsquigarrow \mu(n)$, $\mu:\mathbb{N} \rightsquigarrow M$ er strengt voksende og dermed injektiv.

Knebet er at indhente p med et μ-billede, og det viser sig (lidet overraskende) at $\mu(p)$ kan bruges. Når p på denne måde er indhentet, er det næste kneb at indse, at p så selv må være et μ-billede.

Vi vil gerne vise, at μ også er surjektiv. Til den ende har vi brug for først at indse, at for alle $n \in \mathbb{N}$ er $\mu(n) \geq n$. Dette er øjensynlig sandt for $n = 1$. Antages at $\mu(n) \geq n$ vil $\mu(n+1) > \mu(n) \geq n$, hvorved også $\mu(n+1) \geq n+1$. Induktionsprincippet sikrer, at egenskaben er opfyldt for alle n.

Lad dernæst $p \in M$. S vil $\mu(p) \geq p$. Det påstås nu, at

$$p \in \{\mu(1),\ldots\mu(p)\}.$$

Er $\mu(p) = p$, er dette klart. Ellers er $\mu(p) > p$. Så vil $p \in \{\mu(1),\ldots,\mu(p-1)\}$. Hvis ikke måtte jo $p \in M \setminus \{\mu(1),..\mu(p-1)\}$. Men da $\mu(p) = \min (M \setminus \{\mu(1),\ldots,\mu(p-1)\}$ måtte videre $\mu(p) \leq p$ i strid med, at $\mu(p) > p$. I alt vil $p \in \{\mu(1),\ldots\mu(p)\}$. dvs. der findes et $n \in \mathbb{N}$ ($1 \leq n \leq p$), så at $\mu(n) = p$. Men så er μ surjektiv, altså i alt bijektiv. Men så er M ækvipotent med $\mathbb{N}$.

IV. DE REELLE TAL

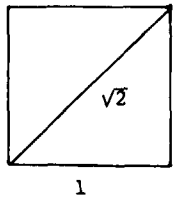
Udvidelse af de rationale tal til de reelle tal

Historisk indledning

De reelle tals historie er ikke langt fra at være matematikkens historie, for matematikkens klassiske discipliner er så snævert forbundet med begrebet om og brugen af de reelle tal, at man knap kan tale om det ene uden at tale om det andet. Der kan derfor kun i et indledende afsnit af denne art være tale om at omtale er par hovedpunkter i det historiske forløb.

Allerede babylonerne var inde på livet af (nogle af) de reelle tal, men uden at opdage det, dvs. uden at opdage at de adskiller sig fra naturlige og rationale tal. Babylonernes behandling af 2. gradsligningen (hvor de nåede meget langt) førte dem ud i kvadratrodsuddragning, også i sammenhænge hvor roduddragningen leder til irrationale tal. Når det ikke gav dem nogen problemer, var det fordi deres interesse for matematik i mindre grad var filosofisk end teknisk/praktisk. Den deraf følgende resultatorientering bevirkede, at roduddragninger som ikke uden videre gav et endegyldigt og eksakt facit, blev foretaget med tilnærmelse, ofte med en nøjagtighed der var fuldt tilstrækkelig til alle den tids beregningsformål. F.eks. angav babylonerne $\sqrt{2}$ som $1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3} \approx 1.41421297$, hvor den "rigtige" tilnærmelsesværdi med dette antal decimaler er 1.41421356.

En geometrisk fortolkning af dette resultat er, at i et kvadrat med siden 1 kan diagonalen (der har længden $\sqrt{2}$) og siden ikke måles med den samme enhed, dvs. der findes ikke noget linjestykke, der går et helt antal gange op i både siden og diagonalen (uden at efterlade en rest). De to stykker er inkommensurable. Det fik grækerne til at slutte at der ikke findes noget tal, der måler diagonalen i dette kvadrat. Mere generelt drog de den vidtgående konsekvens, at tallene ikke egner sig som grundlag for en beskrivelse af alle dele af virkeligheden. De grundlagde derfor deres geometri på betragtninger som undgik talmæssige beskrivelser, men bestod i dybsindige og kunstfærdige operationer med abstrakte størrelser og størrelsesforhold. Dette skridt



som fik gennemgribende betydning for matematikkens senere udvikling kan vi desværre ikke komme nærmere ind på her.

Imidlertid forlod jo kvantitativ omgang med virkeligheden ikke dermed matematikkens historie, heller ikke hos grækerne. Når det ikke gjaldt om at lægge et logisk og filosofisk tilfredsstillende fundament for en matematikkens videnskabsteori, men om at bruge matematikken til forskellige, herunder naturvidenskabelige, formål, drømte heller ikke grækerne om at undgå tallene. Men på grund af de politiske og kulturelle omvæltninger i Europa hen igennem det første årtusind af vor tidsregning forsvandt avanceret matematik groft sagt ud af den europæiske scene indtil middelalderen. Den forsvandt derimod ingenlunde ud af verdenshistorien. Tværtimod skete der i Kina, Indien og Arabien en omfattende opbygning af dele af matematikken, først og fremmest af dens aritmetisk-algebraiske sider (ordet algebra er sådeles af arabisk oprindelse). Da disse kulturers landvindinger (formidlet gennem araberne) blev opdaget og videreført i Europa i den tidlige middelalder overtoges et højtudviklet apparat, som bl.a. indebar en hel del roduddragning, som kunne udføres med vilkårlig nøjagtighed. De "arabiske metoder" gav at magtfuldt redskab, som man simpelthen ikke kunne afstå fra at benytte sig af, selv om der måtte være filosofiske ugler i mosen. At der var det blev nemlig klart om ikke før (f.eks. ved læsning af Platons dialoger, navnlig Theaitetos) så ved genopdagelsen i 1100-tallet af den antikke græske matematik, frem for alt Euklid. Disse tekster havde, skønt bortkommet/glemt i Europa, overlevet og sat frugt i arabisk kultur og i arabisk oversættelse. De blev "tilbageoversat" til latin og græsk i løbet af årene 1200-1500.

Anfægtelserne gjaldt de irrationale tals eksistens. Ved irrationale tal tænktes på den tid udelukkende på tal fremstillet af rodudtryk af rationale tal. Et godt billede af dilemmaet får man af dette citat fra Michael Stifel's (1487?-1567) værk Arithmetica integra (1544):

"Med rette bliver der om de irrationale tal disputeret om de er sande tal eller kun fiktive. Thi ved beviser om de geometriske figurer har de irrationale tal stadig succes , dér hvor

de rationale tal lader os i stikken, og de beviser netop det som de rationale tal ikke kan bevise, i hvert fald ikke med de bevismidler de byder os. Vi bliver altså foranlediget, ja tvunget, til at medgive at de virkelig eksisterer, nemlig på grund af deres virkninger, som vi møder som virkelige, sikre og stående fast.

Men andre grunde foranlediger os til den modsatte påstand, at vi nemlig må bestride at de irrationale tal er tal. Når vi nemlig forsøger at underkaste dem tælling og at sætte dem i forhold til de rationale tal, finder vi at de hele tiden undslipper os, så at ingen af dem lader sig fatte nøjagtigt. Vi bemærker dette ved opløsningen af dem, som jeg nedenfor på passende sted skal vise.

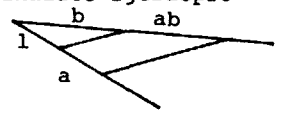
..

Men noget kan ikke kaldes et sandt tal, for hvilket der ingen nøjagtighed gives, og som ikke har bekendte forhold til sande tal. Ligesom et uendeligt tal ikke er noget tal, så er et irrationalt tal ikke noget sandt tal, fordi de så at sige er skjult under en tåge af uendelighed (tilnærmelsesoperationen, m.a.), og forholdet mellem et irrationalt tal og et rationalt er dog ikke mindre ubestemt end det mellem et uendeligt og et endeligt."

I løbet af renæssancen udmøntedes mere og mere forestillingen om de reelle tal som værende tæt forbundet med det såkaldte kontinuum. Stevin (1548-1620) siger: "Tal er det ved hvilket størrelsen af enhver ting kan forklares." Og videre: "Tallet er for størrelsen nærmest som fugtigheden for vandet. Thi som denne udstrækker sig i det hele og i enhver del af vandet, så udstrækker det til en størrelse tilordnede tal sig i hele størrelsen og enhver del. Og som en kontinuerlig vandmængde modsvarer en kontinuerlig fugtighed, så svarer en kontinuerlig størrelse til et kontinuerligt tal." Newton (1643-1727) sætter det således op: "Ved 'tal' forstår vi ikke blot en mængde af enheder, men snarere det abstrakte forhold mellem en vilkårlig størrelse og en anden størrelse af samme natur, der antages som enhed. Det er af trefoldig art: helt, brudent og irrationalt; helt hvis enheden måler det (dvs. går op i det, m.a.), brudent hvis en del af enheden som måler denne enhed flere

gange, måler det, irrationalt hvis det er inkommensurabelt med enheden." (Dette er i virkeligheden en moderne formulering af Eudoxos' proportionslære, som den indgår i Euklid's elementer.)

Men selv om man kunne danne sig intuitive forestillinger om de reelle tal som et kontinuum, var der stadig problemer med at tillægge dem en håndgribelig eksistens. I sin grundlæggelse af den analytiske geometri foretog Descartes (1596-1650) en identifikation mellem de reelle tal og en ret linje, hvorpå der er givet en enhed, altså en tallinje. Derved bliver et reelt tal identisk med et linjestykke. Spørgsmålet er så hvordan man kan indføre algebraiske operationer på sådanne linjestykker. Descartes besvarede dette spørgsmål ved inddragelsen af en række klassiske geometriske konstruktioner. F.eks. er produktet af to linjestykker a og b den såkaldte fjerdeproportional til a og b, jfr. hosstående figur.



I perioden indtil begyndelsen af 1800-tallet grundlagdes, udvikledes og udnyttedes den ny matematiske disciplin, infinitesimalregningen, i et sådant tempo og med en sådan succes, at grundlagsproblemer i den ende af matematikken simpelthen ikke fik fodfæste på dagsordenen. Den derved forbundne omgang med de reelle tal bidrog til at slå deres eksistensberettigelse såvel som deres praktiske uomgængelighed fast med syvtommersøm.

Men hvad med deres eksistens? Som led i den begyndende afklaring af matematikkens grundlag som fandt sted i begyndelsen af 1800-tallet, bl.a. i kølvandet på infinitesimalregningens fremskridt, blev også dette spørgsmål taget op. Et incitament var dybere studier over grænseovergange som blev gennemført af bl.a. Bolzano (1781-1848) og Cauchy (1789-1857). I Bolzano's bevis for sætningen om at en kontinuert funktion på et afsluttet interval [a,b] må antage værdien 0 i mindst ét punkt, hvis f(a) og f(b) har modsat fortegn, opereres med en fortsat halvering af intervaller, startende med [a,b] selv. Pointen i beviset er så, at da intervallængden går mod 0, må interval-

lerne snævre sig sammen om ét tal. Men med hvilken ret kan vi egentlig sige, at der findes et sådant tal fælles for alle intervallerne? Bolzano formulerede dette som et princip, og foretog bl.a. på dets grundlag en opbygning af talsystemet. Cauchy var inde på lignende tanker, da han formulerede sit almindelige konvergensprincip, der i løs formulering siger, at hvis en talfølges elementer alle kan komme vilkårligt tæt på hinanden, blot man går langt nok ud i følgen, vil følgen have et tal som grænseværdi. Også for Cauchy var der tale om et ubevist princip, et aksiom. Et andet incitament var det forhold, at de komplekse tal kunne forstås som par af reelle tal. Denne forståelse blev alment accepteret i 183o'erne, men indebar at Sorteper gik videre til forståelsen af de reelle tal.

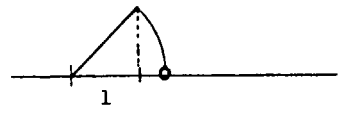
I resten af det 19. århundrede indgår så afklaringen af de reelle tals status i arbejdet med matematikkens grundlag. Der gives en række forskellige forslag til, hvordan de reelle tal kan konstrueres ud fra de rationale, og derved opnå eksistens. Weierstrass (1815-1897) foretog en opbygning baseret på intervalindsnævringer, Dedekind én baseret på de såkaldte snit, mens Méray (1835-1911) og Cantor uafhængigt af hinanden tager udgangspunkt i at tillægge enhver såkaldt fundamentalfølge en grænseværdi. Også andre bud har været givet, bl.a. af Hilbert (1862-1943), der foreslog en aksiomatisk, ikke konstruktiv, fundering af de reelle tal. Det viser sig, at disse bidrag, skønt meget forskellige af ydre, fører til det samme resultat, dvs. det er - i en passende fortolkning - "det samme" talområde kommer ud af dem alle.

I den opbygning vi skal give, følger vi Méray's og Cantor's spor. Lad os inden vi tager rigtigt fat se nærmere på situationen.

I den hidtil foretagne skridtvise udvidelse af talsystemet har hvert skridt været karakteristisk ved, at visse nærliggende opgaver ikke har kunnet løses i det indtil da etablerede talsystem, men har kunnet løses i det der fremgik af udvidelsen.

De opgaver der førte til konstruktionen af de hele og de rationale tal har alle været af algebraisk art: Inden for mængden af naturlige tal kan ikke enhver subtraktionsopgave løses, eller hvad der kommer ud på det samme, ikke enhver ligning af formen $a + x = b$, $a,b \in \mathbb{N}$ har en løsning i $\mathbb{N}$. Inden for de hele tal kan ikke enhver divisionsopgave løses, eller hvad der kommer ud på det samme, ikke enhver ligning af formen $ax = b$, $a,b \in \mathbb{Z}$, $a \neq o$, har en løsning i $\mathbb{Z}$. Derimod kan alle algebraiske opgaver af denne type (division med o selvfølgelig undtaget) løses inden for $\mathbb{Q}$, forsynet med + og $\cdot$, der jo er et legeme.

Den udvidelse af det rationale talområde vi nu skal foretage, er ikke udelukkende styret af behovet for at kunne løse visse ligninger, selv om heller ikke mængden af rationale tal rummer muligheder for at løse enhver ligning, f.eks. ikke ligningen $x^2 = 2$. Formålet med at udvide de rationale tals legeme er at "plombere hullerne" i mængden af rationale tal. Disse huller opstår på flere måder, hvoraf problemet med at løse en ligning som den omtalte fremviser én. Det samme problem kan gives en geometrisk iklædning, som understreger "hulbilledet". Vi betragter tallinjen med en given enhed 1, og opsøger det linjestykke, der er diagonalen i kvadratet med siden 1. Anbringer vi dette linjestykke på tallinjen ud fra begyndelsespunktet på denne, svarer linjestykket(s andet endepunkt) ikke til noget rationalt tal, jfr. tidligere bemærkninger i dette afsnit. I en anden synsmåde opstår hullerne ved at visse følger, som i intuitiv forstand "burde" nærme sig et tal, ikke gør det inden for $\mathbb{Q}$. Ser vi f.eks. på følgen



$$1 + \frac{1}{1!},\ 1 + \frac{1}{1!} + \frac{1}{2!},\ \ldots,\ 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!},\ \ldots,$$

hvor vi sætter

$$a_n = 1 + \frac{1}{1!} + \ldots + \frac{1}{n!},\ n \in \mathbb{N},$$

er det klart at $(a_n)_n$ er strengt voksende, da der i hvert skridt lægges noget positivt til. På den anden side er $(a_n)_n$ begrænset opadtil, f.eks. af tallet 3. Vi har nemlig dels

at $n! = 1\cdot2\cdot3\ldots n \geq 1\cdot2\cdot2\ldots2 = 2^{n-1}$, dels at

$$a_n = 1 + \frac{1}{1!} + \ldots + \frac{1}{n!} \leq 1 + \frac{1}{2^0} + \frac{1}{2^1} + \ldots + \frac{1}{2^{n-1}} =$$

$$1 + \frac{1-(\frac{1}{2})^n}{1-\frac{1}{2}} \leq 1 + \frac{1}{1-\frac{1}{2}} = 3.$$

Det at $(a_n)_n$ på den ene side er strengt voksende og på den anden side opadtil begrænset, kunne lede til en formodning om, at $(a_n)_n$ burde nærme sig en rational grænseværdi (alle a_n-erne er rationale). Man kan endvidere ret let vise, at der til ethvert element $r \in \mathbb{Q}_+$ findes et n_o, så at for $m,n \geq n_o$ gælder $|a_m - a_n| < r$. Dette betyder løst sagt, at "langt ude i følgen er a_m og a_n vilkårligt tætte på hinanden". Men faktisk findes der ikke noget rationalt tal, som a_n kommer vilkårligt tæt på, langt ude. (Man kan vise, at $a_n \to e$, hvor e er grundtallet for den naturlige eksponentialfunktion, og at $e \notin \mathbb{Q}$).

Hensigten med det følgende er at udvide $\mathbb{Q}$ til en mængde, hvori der ikke findes sådanne "huller". Vi har hermed formuleret os en opgave fra analysen, dvs. et problem vedrørende grænseovergange. Imidlertid ønsker vi, at den mængde der skal konstrueres som udvidelse af mængden af rationale tal, på naturlig måde kan udstyres med mindst de samme algebraiske egenskaber som $\mathbb{Q}$, dvs. den skal organiseres som et ordnet legeme.

Lidt upræcist ønsker vi altså at konstruere et ordnet legeme, hvori mængden af rationale tal forsynet med +, · og < kan opfattes som et ordnet dellegeme, og hvori enhver følge som opfylder "for et vilkårligt $r \in \mathbb{Q}_+$ findes et skridt hnsides hvilket forskellen (numerisk) mellem to vilkårlige elementer er mindre end r" har en grænseværdi. Dette ønske skal vi nu skride til at realisere.

Ved L_+ forstås selvfølgelig $L_+ = \{\ell \in L \mid \ell > o\}$.

Ofte kaldes fundamentalfølger for Cauchy-følger.

Vi ser at egenskaben (1) er den som følgen $(a_n)_n$,

$$a_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!},\ n \in \mathbb{N}$$

i indledningsafsnittet postuleredes at besidde. At dette faktisk er tilfældet, fremgår at det for $m > n$ gælder, at

$$|a_m - a_n| = \frac{1}{(n+1)!} + \ldots + \frac{1}{m!} \leq \frac{1}{2^n} + \ldots + \frac{1}{2^{m-1}} = (\tfrac{1}{2})^n \frac{1-(\tfrac{1}{2})^{m-n}}{1-\tfrac{1}{2}}$$

$$= (\tfrac{1}{2})^{n-1}(1-(\tfrac{1}{2})^{m-n}) \leq \frac{1}{2^{n-1}},$$

som er mindre end ε for de n (og m) som opfylder, at $\frac{1}{2^{n-1}} < \varepsilon$, altså alle n (og m) fra et vist trin.

Læg mærke til at ε i (1) og (2) skal hentes fra L_+, og ikke som normalt i tekster om klassisk analyse, fra de positive reelle tal, R_+. Dette skyldes selvsagt, at vi endnu ikke har R til rådighed!

Læg i øvrigt mærke til, at forskellen mellem (1) og (2) bl.a. er, at (1) udtaler sig om , at langt ude i følgen kommer elementerne tæt på hinanden, mens (2) udtaler sig om, at de langt ude kommer tæt på ét bestemt element i L (et element som ingenlunde selv behøver at være element i følgen). Det er desuden vigtigt at holde sig for øje, at spørgsmålet om hvorvidt en følge er en fundamentalfølge (resp. er konvergent) alene angår dens haler, altså dens elementer fra et vist trin. Hvis nemlig $(a_n)_n$ er en fundamentalfølge (resp, er konvergent), vil enhver følge $(b_n)_n$, der stemmer overens med $(a_n)_n$ fra et vist trin være en fundamentalfølge (resp. være konvergent med samme grænsepunkt som a). (Kontrollér selv dette ud fra definitionerne (1) og (2)).

Alment om ordnede legemer

Vi har brug for at lægge ud med at se nærmere på visse forhold i ordnede legemer i almindelighed. De resultater vi opnår vil dels blive benyttet på de rationale tals legeme, dels på legemer som "kandiderer til posten som mængden af reelle tal".

I kapitel III så vi, at i ethvert ordnet legeme $(L,+,\cdot,<)$ kan der defineres en numerisk værdi ved

$$|a| = \begin{cases} a, \text{ hvis } a \geq o \\ -a, \text{ hvis } a \leq o \end{cases}, \quad a \in L.$$

Vi fremsætter nu en almen definition, idet vi minder om, at der ved en følge fra en mængde M forstås en afbildning $a: \mathbb{N} \sim M$, og om at en sådan afbildning specificeres ved skrivemåden $(a_1,a_2,\ldots)$ eller kort $(a_n)_n$, hvor $a_n = a(n)$, $n \in \mathbb{N}$. Mængden af følger fra M betegnes med skrivemåden $M^{\mathbb{N}}$.

Definition: Lad $(L,+,\cdot,<)$ være et ordnet legeme. En følge $(a_n)_n$ fra L kaldes en fundamentalfølge, hvis

$$(1)\ \forall \varepsilon \in L_+\ \exists n_o \in \mathbb{N}\ \forall m,n \in \mathbb{N}\colon m,n \geq n_o \Rightarrow |a_m - a_n| < \varepsilon.$$

Det fænomen, at en følge fra L nærmer sig vilkårligt tæt til et element i L defineres på følgende måde:

Definition: En følge $(a_n)_n$ fra et ordnet legeme $(L,+,\cdot,<)$ siges at være konvergent, hvis der findes et $a \in L$, så at

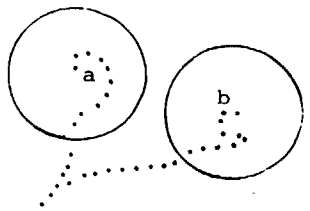
$$(2)\ \forall \varepsilon \in L_+\ \exists n_o \in \mathbb{N}\quad \forall n \in \mathbb{N}\colon n \geq n_o \Rightarrow |a_n - a| < \varepsilon.$$

Hvis (2) er opfyldt kaldes a et grænsepunkt for $(a_n)_n$, og vi skriver $a_n \to a$ for $n \to \infty$.

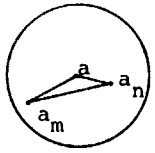
Det ses, at selve definitionen af konvergens indeholder, at der findes en kandidat til posten som grænsepunkt. For at kunne godtgøre, at en given følge er konvergent må man derfor påvise eksistensen af et grænsepunkt.

Der gælder et par sætninger, som er vigtige, men lette at vise:

Idéen i beviset er, at når a og b er forskellige må der om henholdsvis a og b findes omegne, der er disjunkte (se figuren). Og hvis følgen skal være konvergent mod både a og b, må der findes to trin, så at samtlige elementer fra det ene trin at regne ligger i omegnen om a, og samtlige elementer fra det andet trin at regne ligger i omegnen af b. Derved må samtlige elementer længere ude end begge trin ligge i begge omegne. Men de er disjunkte, så det kan ikke lade sig gøre.



Sætningen fortæller, at det er mindst lige så svært at være en konvergent følge, som at være en fundamentalfølge. Beviset beror på den idé - jvf. figuren - at når samtlige elementer fra et vist trin ligger tæt på et bestemt element, må de ligge "halvt så tæt" på hinanden.



$|a_m - a_n| \leq |a_m - a| + |a - a_n|$

Sætning IV.1 Hvis $(a_n)_n$ er en konvergent følge i det ordnede legeme $(L,+,\cdot,<)$ har $(a_n)_n$ ét og kun ét grænsepunkt.

Bevis:

Antag, at $(a_n)_n$ har både a og b som grænsepunkt, hvor $a \neq b$. Så er $|a - b| > 0$. Sættes $\varepsilon_o = \frac{1}{2}|a - b|$ vil $0 < \varepsilon_o < |a - b|$. Da $a_n \to a$ og $a_n \to b$ for $n \to \infty$, findes et $n_o \in \mathbb{N}$ og et $n_1 \in \mathbb{N}$, så at

$$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow |a_n - a| < \tfrac{1}{2}\varepsilon_o$$

og

$$\forall n \in \mathbb{N}: n \geq n_1 \Rightarrow |a_n - b| < \tfrac{1}{2}\varepsilon_o.$$

Det betyder, at for $n \geq \max\{n_o, n_1\}$ vil både

$$|a_n - a| < \tfrac{1}{2}\varepsilon_o \text{ og } |a_n - b| < \tfrac{1}{2}\varepsilon_o,$$

og dermed

$$|a - b| \leq |a_n - a| + |a_n - b| < \varepsilon_o.$$

Da altså både $|a - b| < \varepsilon_o$ og $|a - b| > \varepsilon_o$, hvilket er i strid med ordningens trichotymi, fremstår en modstrid, der skyldes antagelsen om a's og b's forskellighed. Hermed er sætningen bevist.

Sætning IV.2. Hvis en følge er konvergent i det ordnede legeme $(L,+,\cdot,<)$ er den også en fundamentalfølge.

Bevis:

Lad $(a_n)_n$ være konvergent med grænsepunkt $a \in L$, og lad $\varepsilon \in L_+$ være givet. Så findes i kraft af konvergensen et n_o i $\mathbb{N}$, så at

$$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow |a_n - a| < \tfrac{1}{2}\varepsilon.$$

Er derefter $m,n \geq n_o$ vil

$$|a_m - a| < \tfrac{1}{2}\varepsilon \text{ og } |a_n - a| < \tfrac{1}{2}\varepsilon,$$

hvorfor

$$|a_m - a_n| \leq |a_m - a| + |a_n - a| < \varepsilon.$$

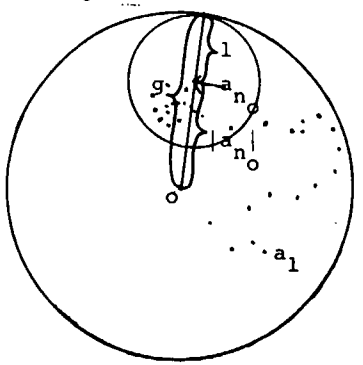
Altså vil for alle $m,n \geq n_o$

$$|a_m - a_n| < \varepsilon. \quad \text{Q.E.D.}$$

Sætningen udtrykker, at en fundamentalfølge ikke kan komme vilkårligt langt omkring i landskabet. Idéen i beviset er, at til et givet ε (f.eks. = 1) findes et trin n_o, så at alle elementer ligger tættere end ε på a_{n_o}.
Og da elementerne

$$a_1, \ldots a_{n_o-1}$$

kun udgør en endelig skare, er hele følgen begrænset.



Heraf ses, at $c(a_n)_n = (c)_n(a_n)_n$, hvor $(c)_n$ er den konstante følge bestående af lutter c'er.

Sætning IV.3. Enhver fundamentalfølge i et ordnet legeme $(L,+,\cdot,<)$ er begrænset, dvs. der findes et $g \in L$, så at

(3) $\forall n \in \mathbb{N}: |a_n| \leq g$.

Bevis:

Da $(a_n)_n$ er en fundamentalfølge findes et $n_o \in \mathbb{N}$, så at

$$\forall m,n \in \mathbb{N}: m,n \geq n_o \Rightarrow |a_n - a_m| < 1$$

(svarende til $\varepsilon = 1$). Specielt gælder, at

$$\forall n \in \mathbb{N}: n \geq n \Rightarrow |a_n - a_{n_o}| < 1.$$

Men så vil for alle $n \geq n_o$

$$|a_n| = |(a_n - a_{n_o}) + a_{n_o}| \leq |a_{n_o} - a_n| + |a_{n_o}| < 1 + |a_{n_o}|.$$

For $n \leq n_o$ vil så meget mere

$$|a_n| \leq \max\{|a_o|, |a_1|, \ldots |a_{n_o}|, 1 + |a_{n_o}|\},$$

hvoraf følger, at med $g = \max\{|a_o|, |a_1|, \ldots |a_{n_o}|, 1 + |a_{n_o}|\}$ vil

$$\forall n \in \mathbb{N}: |a_n| \leq g,$$

hvilket beviser sætningen.

På en naturlig måde defineres nu to kompositioner + og $\cdot$ i $L^{\mathbb{N}}$ ved at vi for vilkårlige $(a_n)_n$ og $(b_n)_n$ i $L^{\mathbb{N}}$ sætter

$$(a_n)_n + (b_n)_n = (a_n + b_n)_n,$$

altså den følge hvis værdi på n er lig $a_n + b_n$, $n \in \mathbb{N}$,
og

$$(a_n)_n \cdot (b_n)_n = (a_n b_n)_n,$$

altså den følge hvis værdi på n er lig $a_n b_n$, $n \in \mathbb{N}$.

Endvidere sætter vi for ethvert $c \in L$

$$c(a_n)_n = (ca_n)_n,$$

altså den følge hvis værdi på n er lig ca_n, $n \in \mathbb{N}$.

Med disse definitioner gælder

Sætning IV.4. (a) Hvis $(a_n)_n$ og $(b_n)_n$ er fundamentalfølger i det ordnede legeme $(L,+,\cdot,<)$ er også $(a_n)_n+(b_n)_n$, $(a_n)_n \cdot (b_n)_n$ og for ethvert $c \in L$ $c(a_n)_n$ fundamentalfølger i L.

I beviset for (4) benyttes på afgørende måde, at enhver fundamentalfølge er begrænset, idet dette forsyner os med en øvre grænse for $|b_m|$ og $|a_n|$, der ikke kommer til at forstyrre den samlede vurdering af differensen.

(b) Hvis $(a_n)_n$ og $(b_n)_n$ er konvergente følger med grænsepunkter henholdsvis a og b i L er også $(a_n)_n+(b_n)_n$ og $(a_n)_n\cdot(b_n)_n$ og for ethvert $c \in L$, $c(a_n)_n$ konvergente følger i L med grænsepunkter henholdsvis a+b, ab og ca.

Bevis:

Hvis $(a_n)_n$ og $(b_n)_n$ er fundamentalfølger har vi for et vilkårligt $\varepsilon \in L_+$, at der findes et n_o og et n_1 i $\mathbb{N}$, så at

$$\forall m,n \in \mathbb{N}: m,n \geq n_o \Rightarrow |a_m - a_n| < \tfrac{1}{2}\varepsilon$$

og

$$\forall m,n \in \mathbb{N}: m,n \geq n_1 \Rightarrow |b_m - b_n| < \tfrac{1}{2}\varepsilon.$$

Så vil

$$\forall m,n \geq \max\{n_o,n_1\} \Rightarrow |(a_m + b_m) - (a_n + b_n)| \leq |a_m - a_n| + |b_m - b_n| < \tfrac{1}{2}\varepsilon + \tfrac{1}{2}\varepsilon = \varepsilon,$$

hvilket viser, at $(a_n)_n + (b_n)_n$ er en fundamentalfølge.

Vi har endvidere

$$(4)\quad |a_m b_m - a_n b_n| = |(a_m - a_n)b_m + (b_m - b_n)a_n| \leq |a_m - a_n||b_m| + |b_m - b_n||a_n|.$$

Da $(a_n)_n$ og $(b_n)_n$ ved at være fundamentalfølger et begrænsede (Sætning IV.3.) findes g_1 og $g_2 > o$, så at

$$\forall n \in \mathbb{N}: |b_n| \leq g_1 \text{ og } |a_n| \leq g_2.$$

Dernæst findes n_o' og n_1' i $\mathbb{N}$, så at

$$\forall m,n \in \mathbb{N}: m,n \geq n_o' \Rightarrow |a_m - a_n| < \frac{\varepsilon}{2g_1}$$

og

$$\forall m,n \in \mathbb{N}: m,n \geq n_1' \Rightarrow |b_m - b_n| < \frac{\varepsilon}{2g_2}.$$

Så vil på grund af (4)

$$\forall m,n \in \mathbb{N}: m,n \geq \max\{n_o',n_1'\} \Rightarrow |a_m b_m - a_n b_n| < \frac{\varepsilon}{2g_1} g_1 + \frac{\varepsilon}{2g_2} g_2 = \varepsilon,$$

hvilket viser, at $(a_n)_n \cdot (b_n)_n$ er en fundamentalfølge.

Hvis $c = o$ er $c(a_n)_n = (o)_n$, der oplagt er en fundamentalfølge. Idet $|ca_m - ca_n| = |c||a_m - a_n|$, vil når $c \neq o$

$$|ca_m - ca_n| < \varepsilon,$$

I et fuldstændigt legeme er pr. definition en følge konvergent, hvis den er en fundamentalfølge. Det betyder i praksis, at i et sådant legeme vil en undersøgelse af konvergens af en given følge ikke kræve tilstedeværelsen af en grænseværdikandidat. Dette er bekvemt, for så vidt som man sjældent vil have en sådan kandidat ved hånden. I stedet kan man nøjes med at foretage en vurdering af afstandene mellem elementerne i følgen.

Undertiden ser man i litteraturen dette faktum om fuldstændigheden omtalt som, at det almindelige konvergensprincip gælder.

Læg mærke til, at denne konstruktion lader sig udføre for ethvert legeme L, altså ikke bare Q. Læg endvidere mærke til, at alle argumenterne i det følgende er holdbare også i en sådan mere almen situation, bortset fra dem der vedrører kommutativiteten af $\cdot$, der kræver, at L selv er kommutativt.

blot $|a_m - a_n| < \frac{\varepsilon}{|c|}$,

hvoraf det umiddelbart fremgår, at $c(a_n)_n$ er en fundamentalfølge.

Hermed er (a) bevist. Beviset for (b) foregår efter helt samme retningslinjer og overlades til læseren. Q.E.D.

Konstruktion af de reelle tals legeme

Det er afgørende, at der ikke i ethvert ordnet legeme gælder det omvendte til Sætning IV.2, altså at enhver fundamentalfølge er konvergent. Det er faktisk netop den skavank ved de rationale tals legeme den nedenfor gennemførte udvidelse skal tjene til at afhjælpe.

Definition: Et ordnet legeme, hvori enhver fundamentalfølge er konvergent kaldes et fuldstændigt legeme.

Betragter vi et rationalt tal r, findes der adskillige følger fra Q der er konvergente med r som grænsepunkt, nemlig f.eks. alle følger $(a_n)_n$, hvor med et eller andet k i $\mathbb{N}$, $a_n = r$ for alle $n \geq k$ (specielt følgen $(a_n)_n$, hvor $a_n = r$ for alle $n \in \mathbb{N}$). Hvis vi lader et rationalt tal repræsentere af mængden af samtlige følger, der konvergerer mod dette tal, har vi kimen til en udvidelse af Q. At én følge repræsenterer samme rationale tal som en anden, kommer nemlig ud på (se Sætning IV.4. at deres differens konvergerer mod o. Et "hul" i Q kan derefter naturligt repræsenteres af mængden af samtlige fundamentalfølger hvis differens med en given fundamentalfølge (som "burde" konvergere i Q men ikke gør det) konvergerer mod o.

I det formelle system går vi frem på følgende måde:

Lad F være mængden af fundamentalfølger fra Q, altså

$$F = \{(a_n)_n \in Q^{\mathbb{N}} \mid (a_n)_n \text{ er en fundamentalfølge}\}.$$

Med kompositionerne + og $\cdot$ indført i $Q^{\mathbb{N}}$ som ovenfor i $L^{\mathbb{N}}$, bliver (F,+,$\cdot$) en kommutativ ring med ételement.

Hvis det legeme L, som konstruktionen tager udgangspunkt i - jvf. side 149 - ikke er kommutativt, kan vi kun slutte, at $(F,+,\cdot)$ er en ring med etelement, ikke at den også er kommutativ.

Når $(F,+,\cdot)$ ikke er en integritetsring, er den selvfølgelig heller ikke et legeme.

At + og · er stabile følger af, at summen og produktet af to fundamentalfølge er en fundamentalfølge. Endvidere er + associativ og kommutativ, da

$((a_n)_n + (b_n)_n) + (c_n)_n = (a_n + b_n)_n + (c_n)_n =$
$((a_n + b_n) + c_n)_n = (a_n + (b_n + c_n))_n = (a_n)_n + (b_n + c_n)_n =$
$(a_n)_n + ((b_n)_n + (c_n)_n)$

og

$(a_n)_n + (b_n)_n = (a_n + b_n)_n = (b_n + a_n)_n = (b_n)_n + (a_n)_n$.

Følgen $0 = (o)_n$ bestående af lutter nuller, altså den konstante afbildning af $\mathbb{N}$ ind i $\{o\} \subseteq \mathbb{Q}$, der åbenbart tilhører F, er tydeligvis neutralt element ved +, da der for ethvert $(a_n)_n \in F$ gælder:

$(a_n)_n + 0 = (a_n)_n + (o)_n = (a_n + o)_n = (a_n)_n$.

Ethvert element $(a_n)_n \in F$ har et inverst ved +, nemlig $-(a_n)_n = (-a_n)_n$.

Argumentationen for at · er associativ og kommutativ forløber helt parallelt med den netop præsenterede for +.

Endvidere er · distributiv m.h.t. +, idet

$((a_n) + (b_n)_n)\cdot(c_n)_n = (a_n + b_n)_n \cdot (c_n)_n = ((a_n + b_n)c_n)_n =$
$(a_n c_n + b_n c_n)_n = (a_n c_n)_n + (b_n c_n)_n = (a_n)_n \cdot (c_n)_n + (b_n)_n \cdot (c_n)_n$.

Følgen $1 = (1)_n$ bestående af lutter 1-er, altså den konstante afbildning af $\mathbb{N}$ ind i $\{1\} \subseteq \mathbb{Q}$, tilhører klart F og er neutralt element ved ·, idet for ethvert $(a_n)_n \in F$

$(a_n)_n \cdot 1 = (a_n)_n \cdot (1)_n = (a_n \cdot 1)_n = (a_n)_n$.

Hermed har vi indset, at $(F,+,\cdot)$ er en kommutativ ring med ételement. Den er imidlertid ikke en integritetsring, idet nulreglen ikke gælder. F.eks. er

$$(a_n)_n \cdot (b_n)_n = 0,$$

hvor

$$a_n = \begin{cases} 1 \text{ for } n = o,1 \\ o \text{ for } n \geq 2 \end{cases}$$

og

$$b_n = \begin{cases} o \text{ for } n = o,1 \\ 1 \text{ for } n \geq 2 \end{cases},$$

hvorved $(a_n)_n$ og $(b_n)_n$ begge tilhører $F \setminus \{0\}$.

Vi skal nu indføre en ækvivalensrelation i $(F,+,\cdot)$, idet vi vil

I disse betragtninger benyttes et par gange Sætning IV.4.

regne to følger for ækvivalente, hvis deres differens er konvergent med o som grænsepunkt (heraf følger selvsagt ingenlunde, at nogen af de to følger selv behøver at være konvergent).

For overskuelighedens skyld udskiller vi først mængden O;

$$O = \{(a_n)_n \in F \mid a_n \to o \text{ for } n \to \infty\} \subseteq F.$$

Elementerne i O kaldes for nulfølger. (Når vi bruger benævnelsen nulfølgen tænker vi altid på følgen bestående af lutter nuller, altså 0.)

Herefter defineres en relation i F ved:

Definition: Ved for vilkårlige $(a_n)_n$ og $(b_n)_n$ i F at fastlægge

$$(5)\quad (a_n)_n \sim (b_n)_n \Leftrightarrow (a_n - b_n)_n \in O$$

defineres en relation $\sim$ i F.

Denne relation $\sim$ er en ækvivalensrelation,

hvilket ses af, at for vilkårlige $(a_n)_n$, $(b_n)_n$ og $(c_n)_n$ i F gælder

$(a_n)_n \sim (a_n)_n$, da $(a_n - a_n)_n = (o)_n \in O$,

af at

$(a_n)_n \sim (b_n)_n \Rightarrow (b_n)_n \sim (a_n)_n$, da $a_n - b_n \to o$ for $n \to \infty$ afstedkommer, at $b_n - a_n = -(a_n - b_n) \to o$ for $n \to \infty$, hvilket viser, at $(b_n - a_n)_n \in O$,

og af at

$(a_n)_n \sim (b_n)_n \wedge (b_n)_n \sim (c_n)_n \Rightarrow (a_n)_n \sim (c_n)_n$, fordi $a_n - b_n \to o$ og $b_n - c_n \to o$ for $n \to \infty$ medfører, at $(a_n - c_n) = (a_n - b_n) + (b_n - c_n) \to o$ for $n \to \infty$, hvilket viser, at $(a_n - c_n)_n \in O$.

Ækvivalensrelationen $\sim$ harmonerer med + og $\cdot$ i F.

Af $(a_n)_n \sim (b_n)_n$ og $(a'_n)_n \sim (b'_n)_n$ sluttes nemlig, da $a_n - b_n \to o$ og $a'_n - b'_n \to$ og for $n \to \infty$, at

$$(a_n + a'_n) - (b_n + b'_n) = (a_n - b_n) + (a'_n - b'_n) \to o \text{ for } n \to \infty,$$

hvilket vil sige, at $((a_n)_n + (a'_n)_n) - ((b_n)_n + (b'_n)_n) \in O$. Men det betyder netop, at $(a_n)_n + (a'_n)_n \sim (b_n)_n + (b'_n)_n$, altså at $\sim$ harmonerer med +.

I det generelle tilfælde bliver $F/\sim$ kun en ring og $(Q^*, +, \cdot)$ ⟶ kun et legeme.

I beviset for at $\sim$ harmonerer med $\cdot$ skal vi benytte, at enhver fundamentalfølge er begrænset. Vi finder

$$a_n a'_n - b_n b'_n = (a_n - b_n)a'_n + b_n(a'_n - b'_n) \to 0 \text{ for } n \to \infty,$$

idet begrænsetheden af $(a'_n)_n$ og $(b_n)_n$ bevirker eksistensen af grænser g og G fra Q_+, så at

$$|a_n a'_n - b_n b'_n| \leq |a_n - b_n| g + |a'_n - b'_n| G \leq \max\{g,G\}(|a_n - b_n| + |a'_n - b'_n|),$$

hvorefter vil til $\varepsilon \in Q_+$ kan finde n_o og $n_1 \in \mathbb{N}$, så at

$$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow |a_n - b_n| < \frac{\varepsilon}{2\max\{g,G\}}$$

og

$$\forall n \in \mathbb{N}: n \geq n_1 \Rightarrow |a'_n - b'_n| < \frac{\varepsilon}{2\max\{g,G\}}.$$

Med disse vurderinger til rådighed slutter vi så, at

$$\forall n \in \mathbb{N}: n \geq \max\{n_o,n_1\} \Rightarrow (|a_n - b_n| + |a'_n - b'_n|) \max\{g, G\}$$

hvilket viser, at $(a_n)_n(a'_n)_n - (b_n)_n(b'_n)_n \in 0$. Vurderingerne undervejs af $|a_n - b_n|$ og $|a'_n - b'_n|$ beroede på at $(a_n - b_n)_n \in 0$ og tilsvarende med $(a'_n - b'_n)_n$.

I alt har vi fundet, at $(a_n)_n(b_n)_n \sim (a'_n)_n(b'_n)_n$, hvilket udtrykker, at $\sim$ harmonerer med $\cdot$.

På grund af harmonien kan kompositionerne + og $\cdot$ overføres til kvotientmængden $F/\sim$, der derved bliver en kommutativ ring med ételement E (klassen der indeholder $1 = (1)_n$), og hvis nulelement er klassen 0 bestående af nulfølgerne. Vi bruger betegnelsen Q^* for $F/\sim$, elementerne i Q^* betegnes med bogstavet Φ, og det element hvis repræsentant er $(a_n)_n \in F$ betegnes med $\Phi_{(a_n)_n}$.

Idet vi også benytter betegnelserne + og $\cdot$ for kompositionerne i Q^*, ønsker vi at vise, at $(Q^*,+,\cdot)$ er et kommutativt legeme. I betragtning af at vi allerede ved, at $(Q^*,+,\cdot)$ er en kommutativ ring med ételement, mangler vi blot at vise, at ethvert element forskelligt fra 0 har et inverst ved $\cdot$.

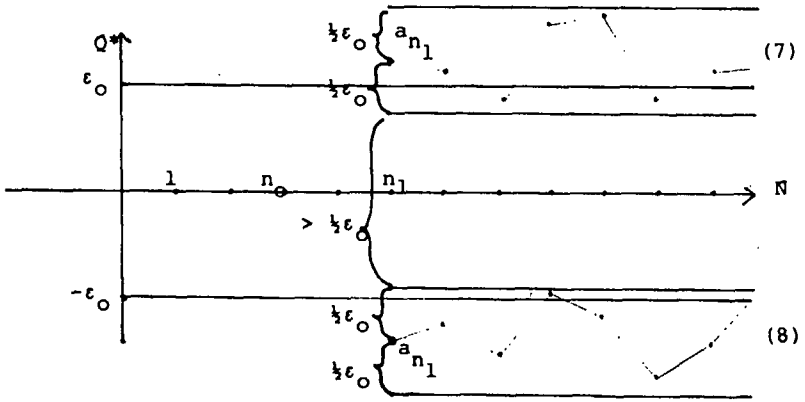
Lad derfor $\Phi_{(a_n)_n}$ være et vilkårligt fra 0 forskelligt element i Q^*, dvs. et element for hvilket $(a_n)_n$ ikke er en nulfølge. Vores opgave er at bestemme et $(b_n)_n \in F$, så at

At vise (6) forudsætter, at $(a_n)_n$ ikke kan have o på alle pladser fra et vist trin; thi havde den det ville jo også følgen $(a_nb_n)_n$ have o på alle pladser fra et vist trin, hvilket ville forhindre (6) i at gælde. Vi må derfor mindst kunne godtgøre, at enhver fundamentalfølge, der ikke er en nulfølge, må have alle sine elementer forskellige fra o fra et vist trin. Dette er en konsekvens af Sætning IV.5., der desuden giver et noget skarpere resultat.

Det kan betale sig at investere lidt energi i at forstå sætningen til bunds. Den bruges uafladeligt i det følgende, idet indførelsen af en ordning på Q* tager udgangspunkt i denne sætning. I løse vendinger siger den, at der for en fundamentalfølge foreligger tre muligheder: enten er den en nulfølge, og hvis ikke er enten alle dens elementer fra et vist trin større end et vist positivt tal, eller også alle mindre end et vist negativt tal.

Bemærk i øvrigt, at hvis $(a_n)_n$ opfylder den ene af (7) eller (8), vil $-(a_n)_n$ opfylde den anden.

For at forstå idéen i beviset må man forstå indholdet i udsagnet (9). Det er at der for ethvert nummer findes et element længere ud i følgen som er numerisk større end et vist ε_o. Sammenholdes nu det med at elementerne fra et vist trin ikke kan afvige (numerisk) fra hinanden end $\frac{1}{2}\varepsilon_o$ ($(a_n)_n$ er jo en fundamentalfølge), må alle elementerne være numerisk større end $\frac{1}{2}\varepsilon_o$ fra et vist trin. Da elementerne skal være tættere på hinanden end $\frac{1}{2}\varepsilon_o$ f.v.t. kan det ikke lade sig gøre at nogle ligger over $\frac{1}{2}\varepsilon_o$ og andre under $-\frac{1}{2}\varepsilon_o$. Altså er kun den ene mulighed til rådighed. Situationen kan illustreres således:



$$E = \Phi_{(1)_n} = \Phi_{(a_n)_n} \cdot \Phi_{(b_n)_n} = \Phi_{(a_nb_n)_n},$$

hvor det er det andet lighedstegn, der her er det interessante. Med andre ord skal vi bestemme $(b_n)_n \in F$, så at

(6) $a_nb_n - 1 \to o$ for $n \to \infty$.

Dette sker ved hjælp følgende vigtige resultat, der også spiller hovedrollen i mange af de kommende argumenter.

Sætning IV.5. Om en fundamentalfølge der ikke er en nulfølge (dvs. $\notin$ O), $(a_n)_n$ gælder ét af to, (7) eller (8), men ikke begge dele:

(7) Der findes et $g \in Q_+$ og et $n_o \in \mathbb{N}$, så at
$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow g < a_n$,
eller

(8) Der findes et $g \in Q_+$ og et $n_o \in \mathbb{N}$, aå at
$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow a_n < -g$.

Bevis:
Det er oplagt, at (7) og (8) ikke kan gælde samtidig, da så samtlige følgens elementer hinsides et vist skridt skulle være både positive (7) og negative (8).

Da $(a_n)_n$ ikke er en nulfølge, må der findes et $\varepsilon_o \in Q_+$, så at

(9) $\forall p \in \mathbb{N}\ \exists n_p \in \mathbb{N}: n_p \geq p \ \wedge\ |a_{n_p}| \geq \varepsilon_o$

(dette er blot negationen af den egenskab der definerer medlemskab af O).

På den anden side er $(a_n)_n$ en fundamentalfølge, hvorfor der findes et $n_o \in \mathbb{N}$, så at

(1o) $\forall m,n \in \mathbb{N}: m,n \geq n_o \Rightarrow |a_m - a_n| < \frac{1}{2}\varepsilon_o$.

Af (9) følger så, med $p = n_o$, at der findes et $n_1 \geq n_o$, så at

$|a_{n_1}| \geq \varepsilon_o$, dvs. (a) $a_{n_1} \geq \varepsilon_o$ eller (b) $a_{n_1} \leq -\varepsilon_o$.

Men så er, på grund af (1o), med n_1 i m's rolle

$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow |a_{n_1} - a_n| < \frac{1}{2}\varepsilon_o$,

eller anderledes udtrykt

$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow -\frac{1}{2}\varepsilon_o + a_n < a_{n_1} < \frac{1}{2}\varepsilon_o + a_n$.

Hvis (a) gælder har vi

Omskrivningerne udnytter, at Q er kommutativt. Hvis vi arbejdede i et ikke-kommutativt legeme, måtte vi gøre lidt flere krumspring:

$$|b_n - b_m| = |a_n^{-1} - a_m^{-1}| = |a_n^{-1}(a_m - a_n)a_m^{-1}| = |a_n^{-1}||a_m - a_n||a_m^{-1}|$$

Desuden skulle vi i stedet vælge n_1, så at

$\forall m,n \in \mathbb{N}: m,n \geq n_1 \Rightarrow |a_m - a_n| < g\varepsilon g$,

således, at vi længere nede ville finde

$|b_n - b_m| < g^{-1}(g\varepsilon g)g^{-1} = \varepsilon$.

$$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow \varepsilon_o \leq a_{n_1} < \tfrac{1}{2}\varepsilon_o + a_n,$$

altså

$$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow a_n > \tfrac{1}{2}\varepsilon_o,$$

og hvis (b) gælder:

$$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow -\tfrac{1}{2}\varepsilon_o + a_n < a_{n_1} \leq -\varepsilon_o,$$

altså

$$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow a_n < -\tfrac{1}{2}\varepsilon_o.$$

Sættes $g = \frac{1}{2}\varepsilon_o$, følger sætningen. Q.E.D.

Med støtte i denne sætning kan vi gå i kast med til $(a_n)_n \in F \setminus 0$ at bestemme en følge $(b_n)_n \in F$, så at (6) er opfyldt:

$$a_n b_n - 1 \to 0 \text{ for } n \to \infty.$$

Lad $g \in Q_+$ og $n_o \in \mathbb{N}$ være bestemt i overenstemmelse med Sætning IV.5. (svarende til (7) eller (8)). Vi sætter nu

$$b_n = \begin{cases} 1 \text{ for } n < n_o \\ 1/a_n \text{ for } n \geq n_o \end{cases},$$

(dette er muligt, da $a_n \neq 0$ for $n \geq n_o$ i kraft af (7) eller (8), og da $(Q,+,\cdot)$ er et legeme). Kan vi vise, at $(b_n)_n$ er en fundamentalfølge, er vores opgave løst, eftersom

$$a_n b_n = \begin{cases} a_n \text{ for } n < n_o \\ 1 \text{ for } n \geq n_o \end{cases}$$

hvilket medfører, at $a_n b_n - 1 \to 0$ for $n \to \infty$.

At $(b_n)_n$ er en fundamentalfølge ses således:

Lad $\varepsilon \in Q_+$. For $m,n \geq n_o$, hvor n_o er det ovenfor bestemte tal, er

$$|b_n - b_m| = |a_n^{-1} - a_m^{-1}| = |a_n^{-1}a_m^{-1}(a_m - a_n)| = |a_n^{-1}a_m^{-1}||a_m - a_n|.$$

Da $|a_m| > g$ og $|a_n| > g$ i kraft af (7) eller (8), er

$$|a_m^{-1}a_n^{-1}| < \frac{1}{g^2} = g^{-2},$$

og da der findes et $n_1 \in \mathbb{N}$, så at

$$\forall m,n \in \mathbb{N}: m,n \geq n_1 \Rightarrow |a_m - a_n| < g^2\varepsilon,$$

vil i alt

$$\forall m,n \in \mathbb{N}: m,n \geq \max\{n_o,n_1\} \Rightarrow |b_n - b_m| < g^{-2}(g^2\varepsilon) = \varepsilon,$$

hvoraf det fremgår, at $(a_n)_n$ er en fundamentalfølge.

Den ordning vi agter at indføre på Q^* , tager udgangspunkt i Sætning IV.5., der jo for enhver fundamentalfølge $(a_n)_n$, der ikke er en nulfølge, skelner mellem to tilfælde, der ikke kan indtræffe samtidig, nemlig (7) og (8). Hvis $(a_n)_n$ er konvergent med grænsepunkt $r \in Q$, gælder åbenbart, at hvis $r \in Q_+$, må tilfælde (7) indtræde, mens tilfælde (8) indtræder, hvis $r \in Q_-$ (da $(a_n)_n \notin 0$, må $r \neq o$).

Eftersom vi i kraft af den isomorfi, som vi senere skal udpege mellem $(Q,+,\cdot)$ og et dellegeme af $(Q^*,+,\cdot)$ identificerer Q med det dellegeme af Q^* som består af de klasser der har konvergente følger (med rational grænseværdi) som deres repræsentanter, er det nærliggende - hvis ordningen på Q^* skal udvide ordningen på Q - at lade den have den egenskab, at hvis for et $r \in Q_+$ $a_n \to r$ for $n \to \infty$, tænker vi på $(a_n)_n$ som positiv, og hvis for et $r \in Q_-$ $a_n \to r$ for $n \to \infty$, tænker vi på følgen som negativ, mens vi selvfølgelig tænker på den som nul, hvis $a_n \to o$ for $n \to \infty$.

Men så har vi indset, at med $(b_n)_n$ defineret som ovenfor mævnt er $(b_n)_n \in F$ og $\Phi_{(b_n)_n}$ invers til $\Phi_{(a_n)_n}$.

Sammenfattende har vi nu godthjort, at $(Q^*,+,\cdot)$ er er kommutativt legeme. Der resterer endnu tre spørgsmål:

1) vi skal have $(Q,+,\cdot)$ indlejret som dellegeme af $(Q^*,+,\cdot)$,
2) vi skal gøre $(Q^*,+,\cdot)$ til et ordnet legeme med en ordning $<_{Q^*}$, der udvider ordningen $<$ fra Q, og
3) vi skal vise, at $(Q^*,+,\cdot,<_{Q^*})$ er et fuldstændigt legeme.

Disse bestræbelser indfries gennem Sætning IV.6., der vises nedenfor. Først skal vi dog have indført en ordning $<_{Q^*}$ på Q^* ved

Definition: Der defineres en relation $<_{Q^*}$ på følgende måde

Lad Φ_1 og Φ_2 være vilkårlige elementer i Q^* med repræsentanter henholdsvis $(b_n)_n$ og $(a_n)_n$ fra F. Så sættes

(11) $\Phi_1 >_{Q^*} \Phi_2 \Leftrightarrow (b_n - a_n)_n$ opfylder (7), (dvs.
$\Leftrightarrow$ der findes et $g \in Q_+$ og et $n_o \in \mathbb{N}$, så at
$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow b_n - a_n > g$.)

For at kunne tillade os at omtale (11) som en definition må vi godtgøre, at hvis $(a'_n)_n$ og $(b'_n)_n$ er andre repræsentanter for henholdsvis Φ_2 og Φ_1, gælder

$$\Phi_{(b_n)_n} >_{Q^*} \Phi_{(a_n)_n} \Leftrightarrow \Phi_{(b'_n)_n} >_{Q^*} \Phi_{(a'_n)_n},$$

eller med brug af (7): følgen $(b_n - a_n)_n$ opfylder (7) hvis og kun hvis $(b'_n - a'_n)_n$ opfylder (7).

At det forholder sig sådan ses således: Lad os antage, at $(b_n - a_n)_n$ opfylder (7). Så findes et $g \in Q_+$ og et $n_o \in \mathbb{N}$, så at

$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow b_n - a_n > g$.

Da $(a'_n)_n \sim (a_n)_n$ og $(b'_n)_n \sim (b_n)_n$, vil $a'_n - a_n \to o$ og $b'_n - b_n \to o$ for $n \to \infty$. Derfor findes n_1 og n_2 i $\mathbb{N}$, så at

$\forall n \in \mathbb{N}: n \geq n_1 \Rightarrow -\frac{g}{3} < a'_n - a_n < \frac{g}{3}$

og

$\forall n \in \mathbb{N}: n \geq n_2 \Rightarrow -\frac{g}{3} < b'_n - b_n < \frac{g}{3}$.

Men så vil for ethvert $n \geq \max\{n_o, n_1, n_2\}$:

$b'_n - a'_n = (b'_n - b_n) + (b_n - a_n) + (a_n - a'_n) > -\frac{g}{3} + g - \frac{g}{3} = \frac{g}{3}$.

Dette viser, at der findes et g' (nemlig $g' = \frac{g}{3}$) og et n'_o

Som ved tidligere tilsvarende lejligheder benyttes 1) til at identificere $(Q,+,\cdot)$ med et dellegeme, $(Q',+,\cdot)$ af $(Q^*,+,\cdot)$.

Ordningen $<$ på Q' defineres ved: $\alpha < \beta \Leftrightarrow r < q$, hvor q og r er de entydigt bestemte elementer i Q, for hvilke $\alpha = \varphi(q)$ og $\beta = \varphi(r)$, og hvor φ er den isomorfi som etableres i kraft af 1).

Ad 2): Hvis i det almene tilfælde L ikke er kommutativt, må (14) suppleres med, at også $\gamma\alpha >_{Q^*} \gamma\beta$.

Ad 3): Dette punkt udtrykker, at vilkårligt tæt på ethvert element i Q^* findes der elementer fra Q.

(nemlig $n_o' = \max\{n_o, n_1, n_2\}$), så at
$\forall n \in \mathbb{N}: n \geq n_o' \Rightarrow b_n' - a_n' > g'$,
hvilket netop udtrykker, at $(b_n' - a_n')_n$ opfylder (7). Da $(b_n - a_n)_n$ og $(b_n' - a_n')_n$ indgår symmetrisk i problemstillingen, kan vi tilsvarende slutte, at hvis $(b_n' - a_n')_n$ opfylder (7) gælder det samme $(b_n - a_n)_n$.

Vi er nu rustet til at vise Sætning IV.6., idet vi fra nu af betegner elementerne i Q^* med små græske bogstaver.

Sætning IV.6. Med legemet $(Q^*,+,\cdot)$ opbygget som ovenfor gælder:

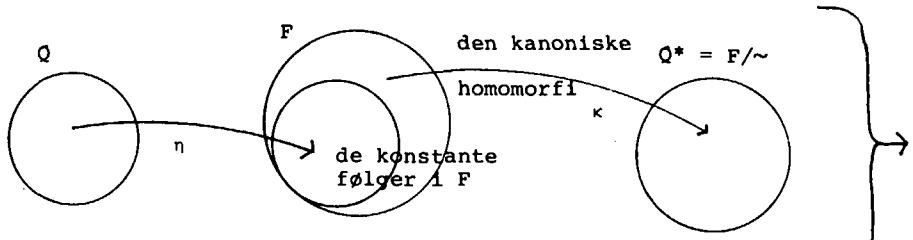
1) Der findes et dellegeme $(Q',+,\cdot)$ af $(Q^*,+,\cdot)$ som er isomorft med $(Q,+,\cdot)$.
2) Den ved definitionen af $<_Q$ bestemte relation på Q er en trichotymisk, irrefleksiv ordningsrelation, der udvider $<$ på Q, dvs. opfylder
   (12) $\forall\alpha,\beta \in Q': \alpha > \beta \Leftrightarrow \alpha >_{Q^*} \beta$,
   hvor $<$ er den ordning på Q', der overføres ved isomorfien fra 1) fra Q.
   Ordningen $<_Q$ harmonerer med kompositionerne + og $\cdot$ i $(Q^*,+,\cdot)$, dvs.
   (13) $\forall\alpha,\beta,\gamma \in Q^*: \alpha >_{Q^*} \beta \Leftrightarrow \alpha + \gamma >_{Q^*} \beta + \gamma$
   og
   (14) $\forall\alpha,\beta \in Q^* \; \forall\gamma \in Q^* \setminus \{o\}: \alpha >_{Q^*} \beta \wedge \gamma >_{Q^*} o \Rightarrow \alpha\gamma >_{Q^*} \beta\gamma$.
3) Q' er tæt i Q^*, dvs.
   (15) $\forall\alpha,\beta \in Q^* \; \exists\gamma \in Q': \alpha < \gamma < \beta$.
4) $(Q^*,+,\cdot,<_{Q^*})$ er et fuldstændigt legeme.

Bevis:
Det skal ikke nægtes, at beviset er en større sag. De fleste punkter er dog nogenlunde simple anvendelser af de foregående udviklinger. For punkt 4)'s vedkommende skal man dog holde tungen lige i munden.

Vi starter med 1):

Afbildningen $\varphi: Q \rightarrowtail Q^*$, defineret ved

$$\varphi(r) = \Phi_{(r)_n}, \text{ for } r \in Q,$$



Idet vi - se figuren - sætter $\varphi(r) = (r)_n$ (= den til r svarende konstante følge), og lader κ være den kanoniske homomorfi fra F til F/~ er $\varphi = \eta o \kappa$. Da η og κ er homomorfier er φ det også.

Læg mærke til, at hvis en fundamentalfølge er ækvivalent med en konvergent følge, er den selv konvergent. (Prøv selv efter).

er en injektiv homomorfi fra Q til Q*.

Thi at φ er en homomorfi følger af, at der for vilkårlige $q,r \in Q$ gælder:

$$\varphi(q+r) = \Phi_{(q+r)_n} = \Phi_{((q)_n + (r)_n)} = \Phi_{(q)_n} + \Phi_{(r)_n} = \varphi(q)+\varphi(r)$$

og

$$\varphi(qr) = \Phi_{(qr)_n} = \Phi_{(q)_n (r)_n} = \Phi_{(q)_n} \cdot \Phi_{(r)_n} = \varphi(q)\varphi(r).$$

Injektiviteten ses af:

Hvis

$$\Phi_{(q)_n} = \varphi(q) = \varphi(r) = \Phi_{(r)_n},$$

er $(q)_n \sim (r)_n$, hvilket betyder, at $q - r \to o$ for $n \to \infty$. Da imidlertid $q - r$ er konstant, kan dette kun indtræffe, hvis $q = r$ (ellers kunne vi ikke til f.eks. $\varepsilon = \frac{1}{2}|q - r|$ bestemme noget n_o så at $|q - r| < \varepsilon$ for alle $n \geq n_o$).

En injektiv homomorfi er en isomorfi ind i billedmængden. Derfor er φ: $Q \sim \varphi(Q) \subset Q^*$ en isomorfi fra legemet $(Q,+,\cdot)$ til dellegemet $(\varphi(Q),+,\cdot)$ af Q* Sætter vi $Q' = \varphi(Q)$, er altså $(Q',+,\cdot)$ et med $(Q,+,\cdot)$ isomorft dellegeme af $(Q^*,+,\cdot)$. Det består af alle de klasser hvis repræsentanter er følger der konvergerer i Q. Hermed er 1) bevist.

Dernæst vender vi os mod 2):

Relationen $<_{Q^*}$ er trichotymisk og irrefleksiv.

Thi for vilkårlige Q*-elementer $\alpha,\beta \in Q^*$ og repræsentanter for dem henholdsvis $(a_n)_n$ og $(b_n)_n$ gælder i kraft af Sætning IV.5. enten at $(b_n - a_n)_n$ er en nulfølge, i hvilket tilfælde $\alpha = \Phi_{(a_n)_n} = \Phi_{(b_n)_n} = \beta$, eller at $(b_n - a_n)_n$ opfylder (7), altså pr. definition (11), at $\beta = \Phi_{(b_n)_n} > Q^* \Phi_{(a_n)_n} = \alpha$, eller som den sidste mulighed, at $(b_n - a_n)_n$ opfylder (8). I dette sidste tilfælde vil $(a_n - b_n)_n$ opfylde (7), hvoraf vi slutter, at $\alpha = \Phi_{(a_n)_n} > Q^* \Phi_{(b_n)_n} = \beta$. Det var trichotymien.

At $<_{Q^*}$ er irrefleksiv følger af, at $(a_n - a_n)_n$ er en nulfølge, hvilket i kraft af Sætning IV.5. er uforenligt med, at følgen opfylder (7) eller (8).

At relationen $<_{Q^*}$ er asymmetrisk, at altså $\alpha > \beta$ forhindrer, at $\beta > \alpha$, er også let at indse,

fordi repræsentanterne $(a_n)_n$ og $(b_n)_n$ for henholdsvis α og β pr. definition ((11)) må opfylde, at $(a_n - b_n)_n$ opfylder (7), hvilket (Sætning IV.5.) er uforeneligt med, at $(b_n - a_n)_n$ opfylder (7).

Det overlades til læseren som en øvelse at indse, at også den til $<_{Q^*}$ svarende refleksive ordning $\leq_{Q^*}$ er en udvidelse af $\leq$, dvs. at der for $\alpha,\beta \in Q'$ gælder: $\alpha \leq \beta \Leftrightarrow \alpha \leq_{Q^*} \beta$.

Transitiviteten af $<_{Q^*}$ godtgøres på følgende måde:

Hvis $\alpha >_{Q^*} \beta$ og $\beta >_{Q^*} \gamma$ og $(a_n)_n$, $(b_n)_n$ og $(c_n)_n$ er repræsentanter for henholdsvis α,β og γ, vil $(a_n - b_n)_n$ opfylde (7), og ligeledes $(b_n - c_n)_n$. Så findes henholdsvis g_o og g_1 i Q_+ og n_o og n_1 i $\mathbb{N}$, så at

$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow a_n - b_n > g_o$

og

$\forall n \in \mathbb{N}: n \geq n_1 \Rightarrow b_n - c_n > g_1$.

Men så vil med $g = g_o + g_1$ og $n_o' = \max\{n_o, n_1\}$

$\forall n \in \mathbb{N}: n \geq n_o' \Rightarrow (a_n - c_n) = (a_n - b_n) + (b_n - c_n) > g_o + g_1 = g$.

Det viser, at $(a_n - c_n)_n$ opfylder (7), at altså $\alpha >_{Q^*} \gamma$.

Det var ordningsrelationsegenskaberne. Så kommer udvidelsesspørgsmålet. For at vise (12) skal vi først slå fast, at $\alpha,\beta \in Q'$ pr. definition af Q betyder, at der findes q og $r \in Q$, så at

$\alpha = \varphi(q) = \Phi_{(q)_n}$ og $\beta = \varphi(r) = \Phi_{(r)_n}$.

Og at $\alpha > \beta$ er ensbetydende med, pr. definition af $<$ i Q', at $q > r$ betragtet i Q.

Argumentet går herefter således: At $\alpha >_{Q^*} \beta$ betyder ((11)), at $(q - r)_n$ opfylder (7). Så findes et $g \in Q_+$ og et $n_o \in \mathbb{N}$, så at for $n \geq n_o$ vil $(q - r) > g$. Heraf følger umiddelbart, da denne ulighed vedrører tal i Q, at $q > g + r > r$, hvorved $q > r$, der netop er betingelsen for at $\alpha > \beta$ i Q'. Vi har dermed vist, at hvis $\alpha >_{Q^*} \beta$ så er også $\alpha > \beta$ i Q'.

Er omvendt $\alpha > \beta$ i Q', dvs, $q > r$, kan vi ved at sætte $g = \frac{1}{2}(q-r)$ og $n_o = 1$ konstatere, at

$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow q - r > g$,

hvilket viser, at $(q-r)_n$ opfylder (7). Men så er $\alpha >_{Q^*} \beta$.

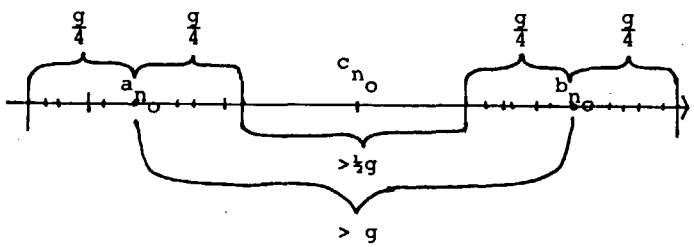
Hermed er (12) vist.

Af punkt 2) tilbagestår harmonibetingelserne. De er enkle at bevise:

Først (13): Lad α,β og γ have repræsentanterne $(a_n)_n$, $(b_n)_n$ og $(c_n)_n$ respektive. Så er $\alpha >_{Q^*} \beta$ ensbetydende med, at $(a_n - b_n)_n$ opfylder (7). Tilsvarende er $\alpha + \gamma >_{Q^*} \beta + \gamma$ ensbetydende med, at følgen $(a_n+c_n)-(b_n+c_n))_n$ opfylder (7). Men denne følge er jo identisk med $(a_n - b_n)_n$, hvorved (13) er godtgjort.

Dernæst (14): Lad $\alpha,\beta \in Q^*$, $\gamma >_{Q^*} o, \gamma \in Q^*$, med repræsentan-

Her benyttes harmoniegenskaberne i $\mathbb{Q}$. $\longrightarrow$



Med denne tallinjeillustration kan bevisgangen anskueliggøres.

ter $(a_n)_n$, $(b_n)_n$ og $(c_n)_n$. Det antages, at $\alpha >_{\mathbb{Q}^*} \beta$, altså at $(a_n - b_n)_n$ er en følge der opfylder (7). Så vil også følgen $(a_nc_n - b_nc_n)_n$ $(= ((a_n - b_n)c_n)_n$ opfylde (7), thi der findes et $g \in \mathbb{Q}_+$ og et $n_o \in \mathbb{N}$, for hvilke

$\forall n \in \mathbb{N}: n \geq n_o \Rightarrow a_n - b_n > g.$

Desuden findes (da $(c_n)_n$ opfylder (7) (γ er antaget $>_{\mathbb{Q}^*} o$)) et $g_1 \in \mathbb{Q}_+$ og et $n_1 \in \mathbb{N}$, så at

$\forall n \in \mathbb{N}: n \geq n_1 \Rightarrow c_n > g_1.$

Dermed vil

$\forall n \in \mathbb{N}: n \geq \max\{n_o, n_1\} \Rightarrow (a_n - b_n)c_n > gg_1,$

hvilket viser, at $(a_nc_n - b_nc_n)_n$ opfylder (7). Men så er $\alpha\gamma = \Phi_{(a_nc_n)_n} >^* \Phi_{(b_nc_n)_n} = \beta\gamma$, og (14) er vist.

Alt i alt er 2) bevist.

Som det næste skal vi nu bevise 3), at $\mathbb{Q}'$ er tæt i $\mathbb{Q}^*$. Lad til den ende α og β være givne elementer i $\mathbb{Q}$, hvor $\alpha < \beta$, og lad $(a_n)_n$ henholdsvis $(b_n)_n$ være repræsentanter for dem. At $\alpha < \beta$ betyder, at $(b_n - a_n)_n$ opfylder (7), altså at der findes et g i $\mathbb{Q}_+$ og et $n_1 \in \mathbb{N}$, så at

$\forall n \in \mathbb{N}: n \geq n_1 \Rightarrow b_n - a_n > g.$

Endvidere er jo $(a_n)_n$ og $(b_n)_n$ fundamentalfølger, hvorfor der findes n_2 og n_3, for hvilke (svarende til $\varepsilon = \frac{g}{4}$)

$\forall m,n \in \mathbb{N}: m,n \geq n_2 \Rightarrow |a_m - a_n| < \frac{g}{4}$

og

$\forall m,n \in \mathbb{N}: m,n \geq n_3 \Rightarrow |b_m - b_n| < \frac{g}{4}.$

Sættes $n_o = \max\{n_1, n_2, n_3\}$ vil

$$\forall m,n \in \mathbb{N}: m,n \geq n_o \Rightarrow \begin{cases} b_n - a_n > g \\ |a_m - a_n| < \frac{g}{4} \\ |b_m - b_n| < \frac{g}{4} \end{cases}.$$

Vi definerer nu en følge $(c_n)_n$ ved for hvert $n \in \mathbb{N}$ at sætte

$c_n = \frac{1}{2}(a_{n_o} + b_{n_o}).$

Følgen $(c_n)_n$ er åbenbart konvergent, da den er konstant, og dermed repræsentant for et element i $\mathbb{Q}'$. Vi påstår, at med $\gamma = \Phi_{(c_n)_n}$ vil

$\alpha < \gamma < \beta,$

hvilket kommer ud på at vise, at både $(c_n - a_n)_n$ og $(b_n - a_n)_n$

Tegnet $||$ kan også uden skade bruges for elementerne i Q' (og dermed i Q), idet jo $<_{Q^*}$ udvider $<$.

Idéen i beviset er som følger:

Den fundamentalfølge $(\alpha_n)_n$ vi betragter i $Q^{*\mathbb{N}}$ tilnærmes (ved hjælp af 3)) i Q^* med elementer fra mængden Q', der jo består af de klasser, hvis repræsentanter er konvergente følger og derfor forventeligt lidt mere fredsommelige end de blotte fundamentalfølger. Ved denne tilnærmelse, der sker led for led, opstår følgen $(\rho_n)_n$, som er en følge i $Q'^{\mathbb{N}}$, og som vises at være en fundamentalfølge. Nu er ethvert ρ_n et billede ved φ af et rationalt tal r_n. Det vises nu, at $\alpha = (r_n)_n$ - som er en følge i $Q^{\mathbb{N}}$ - er en fundamentalfølge, altså et element i F. Clou'et består så i at konstatere - og bevise! - at α er grænsepunkt for $(\alpha_n)_n$.

I øvrigt er bevisførelsen velforsynet med punkter, hvor man skal holde tungen lige i munden. Først skal tilnærmelsen af α_n med ρ_n være bedre, jo større n er, dvs. approksimationsgrænsen η_n skal udgøre en dalende følge i Q^*.

Dernæst er epsilon-rollen forskellig i Q^* og i Q, idet den i Q^* spilles af en klasse af objekter, hvor hvert objekt er en følge fra Q. Approksimationen af α_n med ρ_n gør det dernæst påkrævet at opsøge et ε', der tilhører Q' (og som er mindre end ε), hvad ε jo ikke nødvendigvis gør, for at vi kan udnytte at $(\rho_n)_n$ er en fundamentalfølge. Endelig skal vi til dette ε' finde et η_{n_0}, som er mindre end ε', for derefter at benytte det forhold, at $(\rho_n)_n$ er en fundamentalfølge, til den afsluttende vurdering af differensen $|\alpha-\alpha_m|$.

Se i øvrigt en illustration af forholdene på den næste venstreside.

opfylder (7).

For $n \geq n_o$ gælder, at

$$b_n - c_n = (b_n - b_{n_o}) + (b_{n_o} - \tfrac{1}{2}(a_{n_o} + b_{n_o})) =$$
$$(b_n - b_{n_o}) + \tfrac{1}{2}(b_{n_o} - a_{n_o})$$
$$> -\frac{q}{4} + \frac{q}{2} = \frac{q}{4},$$

og at

$$c_n - b_n = \tfrac{1}{2}(a_{n_o} + b_{n_o}) - a_{n_o} + (a_{n_o} - a_n) = \tfrac{1}{2}(b_{n_o} - a_{n_o}) + (a_{n_o} - a_n)$$
$$\frac{q}{2} - \frac{q}{4} = \frac{q}{2}.$$

Hermed er påstanden vist. Det samme gælder punkt 3).

Egenskaben 3) spiller en afgørende rolle i beviset for 4), der udtrykker at $(Q^*,+,\cdot,<_{Q^*})$ er fuldstændigt. I det følgende refererer tegnet $|\ |$ til den numeriske værdi i Q^*, der udspringer af ordningen i Q^*)jfr. begyndelsen af dette kapitel).

Lad der være givet en vilkårlig fundamentalfølge i Q^*(!), $(\alpha_n)_n$ (husk, at ethvert α_n er en klasse af fundamentalfølger fra Q).

For ethvert $n \in \mathbb{N}$ betragter vi

$$\eta_n = \Phi_{(\frac{1}{n})_k} \quad \text{(der tilhører } Q', \eta_n > o)$$

(altså den klasse der indeholder følgen med $\frac{1}{n}$ konstant på alle pladser). Da Q' er tæt i Q^*, vil der for ethvert $n \in \mathbb{N}$ findes et Q'-element mellem $\alpha_n - \eta_n$ og $\alpha_n + \eta_n$, altså et $\eta_n \in Q'$, så at

(15) $\alpha_n - \eta_n < \rho_n < \alpha_n + \eta_n$.

Vi vil vise, at $(\rho_n)_n$ er en fundamentalfølge. For alle m,n har vi

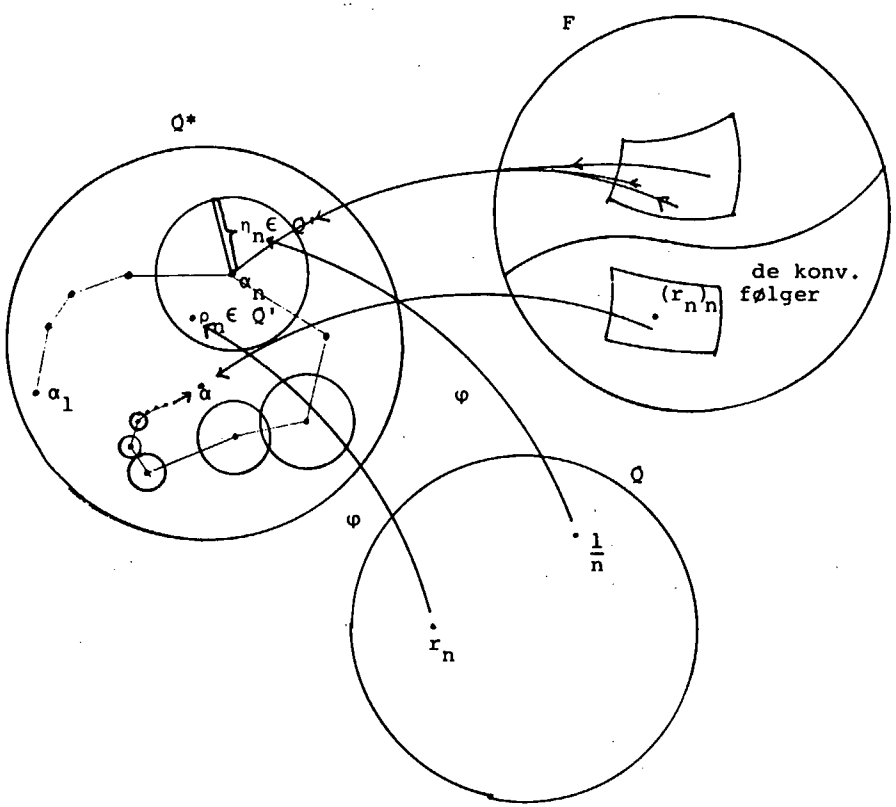
(16) $|\rho_m - \rho_n| = |(\rho_m - \alpha_m) - (\rho_n - \alpha_n) + (\alpha_m - \alpha_n)|$
$\leq |\rho_m - \alpha_m| + |\rho_n - \alpha_n| + |\alpha_m - \alpha_n| \leq \eta_m + \eta_n + |\alpha_m - \alpha_n|$.

Lad dernæst $\varepsilon \in Q'_+$. Da findes, idet Q' via φ, defineret under punkt 1), er isomorf med Q, et $p \in Q$, så at ε har formen

$$\varepsilon = \varphi(p) = \Phi_{(p)_k}.$$

Idet der findes et $n_o \in \mathbb{N}$ - eftersom Q er arkimedisk ordnet - så at $\frac{1}{n_o} < \frac{1}{3}p$, vil for alle $n \geq n_o$

(17) $\eta_n \leq \eta_{n_o} < \frac{1}{3}\varepsilon$,



idet jo følgen $(\frac{1}{n_o} - \frac{1}{n})_k$, der er repræsentant for $\eta_{n_o} - \eta_n$, enten er en nulfølge (nemlig hvis $n = n_o$) eller opfylder (7) (nemlig hvis $n > n_o$), og idet følgen

$$(\tfrac{1}{3}p - \tfrac{1}{n_o})_k,$$

der er en repræsentant for $\frac{1}{3}\varepsilon - \eta_{n_o}$, opfylder (7).

Endvidere er jo $(\alpha_n)_n$ en fundamentalfølge i Q*. Så findes et $n_1 \in \mathbb{N}$, så at

(18) $m,n \geq n_1 \Rightarrow |\alpha_m - \alpha_n| < \frac{1}{3}\varepsilon$.

Sammenfattes (16), (17) og (18), får vi

(19) $m,n \geq \max\{n_o,n_1\} \Rightarrow |\rho_m - \rho_n| < \varepsilon$.

Dermed har vi indset, at følgen $(\rho_n)_n$ er en fundamentalfølge i Q'.

Imidlertid er jo Q' (stadig via φ) isomorf med Q. Det bevirker at der til ethvert $n \in \mathbb{N}$ findes netop ét $r_n \in Q$, for hvilket

$$\eta_n = \varphi(r_n) = \Phi_{(r_n)_k}.$$

Følgen $(r_n)_n$ er en fundamentalfølge i Q. Thi da φ er en ordenstro isomorfi vil det af (19) følge, at for ethvert $p \in Q_+$ vil

$$m,n \geq \max\{n_o,n_1\} \Rightarrow \varphi^{-1}(-\varepsilon) < \varphi^{-1}(\rho_m - \rho_n) < \varphi^{-1}(\varepsilon),$$

og dermed for de samme m,n

$$-p < r_m - r_n < p,$$

hvilket viser, at $(r_n)_n$ er en fundamentalfølge. Da aætså $(r_n)_n$ tilhører F, vil α defineret ved

$$\alpha = \Phi_{(r_n)_n}$$

tilhøre Q*.

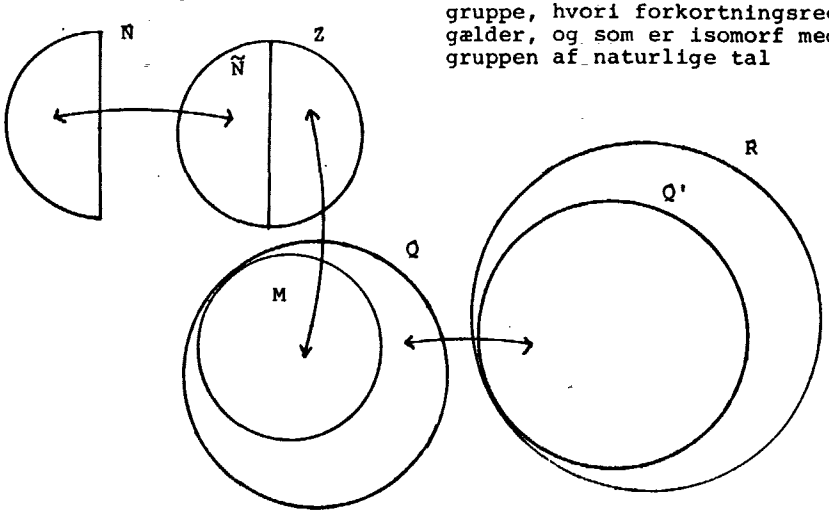
Vi ønsker at vise, at $(\alpha_n)_n$ er konvergent i Q* med α som grænsepunkt. Hermed vil vi have vist, at $(Q^*, +, \cdot, <_{Q^*})$ er et fuldstændigt legeme, målet for hele dette punkt.

For ethvert $m \in \mathbb{N}$ har vi, at

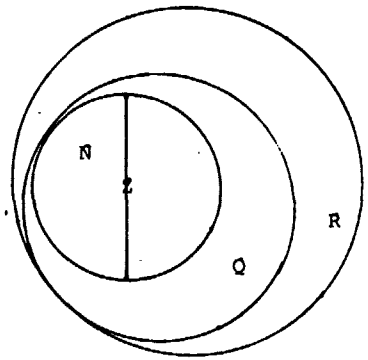
$$|\alpha - \alpha_m| \leq |\alpha - \rho_m| + |\rho_m - \alpha_m| \leq |\alpha - \rho_m| + \eta_m$$
$$= |\Phi_{(r_n)_n} - \Phi_{(r_m)_n}| + \eta_m.$$

Opgaven er her til et givet $\varepsilon \in Q_+^*$ at skaffe et nummer, så at at for m'er hinsides dette nummer er $|\alpha - \alpha_m| < \varepsilon$. Dette kommer efter det netop opnåede ud på at vurdere de to sidste led opad

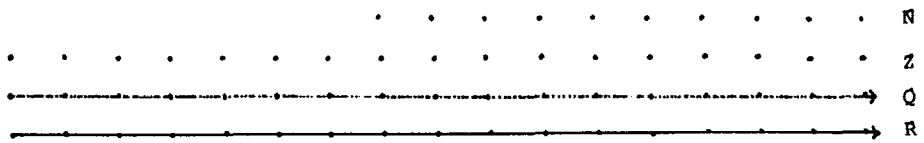
På dette sted ville det måske være på sin plads at se tilbage på den samlede konstruktion. Tag en dyb indånding, og husk, at: de reelle tals legeme er et fuldstændigt ordnet legeme, som er indeholder et dellegeme, der er isomorft med de rationale tals legeme, der på sin side indeholder en delring, som er isomorf med ringen af de hele tal, der indeholder en kommutativ halvgruppe, hvori forkortningsreglerne gælder, og som er isomorf med halvgruppen af naturlige tal



I praksis og til daglig opfatter vi hierarkiet af strukturer og indledjringer som én mængde.
I bolleillustration:



I tallinjeillustration:



ved tilpas små grænser. Vurderingen af η_m gennemføres først.

Da Q' er tæt i Q* findes et $\varepsilon' \in Q'_+$, så at $(o <)\ \varepsilon' < \varepsilon$. Til dette ε' findes et n'_o, så at $\eta_{n'_o} < \frac{1}{2}\varepsilon'$. Det bevirker, at for $m \geq n'_o$ vil

$$\eta_m \leq \eta_{n'_o} < \tfrac{1}{2}\varepsilon'.$$

Hvad leddet $|\Phi_{(r_n)_n} - \Phi_{(r_m)_n}|$ angår, går vi således frem:
Følgen $(r_n)_n$ er en fundamentalfølge i Q. Så findes et n'_1 i N, så at

$$m,n \geq n'_1 \Rightarrow |r_m - r_n| < \frac{1}{n'_o},$$

der også kan udtrykkes:

for ethvert $m \geq n'_1$ vil for ethvert $n \geq n'_1$

$$r_m - \frac{1}{n'_o} < r_n < r_m + \frac{1}{n'_o}.$$

Det viser at alle leddene i de to følger $(r_n - (r_m - \frac{1}{n'_o}))_n$ og $((r_m + \frac{1}{n'_o}) - r_n)_n$ for $n \geq n'_1$ (og forudsat at $m \geq n'_1$) er strengt positive. Men så kan de ikke opfylde (8), hvorfor de må være enten nulfølger eller opfylde (7) (Sætning IV.5. nok engang). Det giver, at

$$-\eta_{n'_o} \leq \Phi_{-(\frac{1}{n'_o})} \leq \Phi_{(r_n)_n - (r_m)_n} \leq \Phi_{(\frac{1}{n'_o})} = \eta_{n'_o},$$

eller m.a.o., da $\Phi_{(r_n)_n - (r_n)_m} = \Phi_{(r_n)_n} - \Phi_{(r_n)_m}$,

$$|\Phi_{(r_n)_n} - \Phi_{(r_n)_m}| \leq \eta_{n'_o} \leq \tfrac{1}{2}\varepsilon'$$

Sammenholdes de to vurderinger, får vi:

$$\forall m \in N: m \geq n'_o \Rightarrow |\alpha - \alpha_m| \leq \tfrac{1}{2}\varepsilon' + \tfrac{1}{2}\varepsilon' = \varepsilon' < \varepsilon,$$

hvorved det er bevist, at $\alpha_m \to \alpha$ for $m \to \infty$. Det var punkt 4)

Hermed er Sætning IV.6. bevist.

Det er på dette grundlag klart, at vi uden videre kan indføre den til $<_{Q^*}$svarende refleksive ordning $\leq_{Q^*}$på Q^*. Den bliver total og harmonerer på passende måde med + og · i Q^*.

Det fuldstændige legeme $(Q^*,+,\cdot,<_{Q^*})$ kaldes de reelle tals legeme, og elementerne deri kaldes reelle tal. I kraft af punkt 1) opfattes de rationale tals legeme som et dellegeme af de reelle tals legeme, og eftersom 2) tillader os at opfatte $<_{Q^*}$som en udvidelse af ordningen < på Q, vil vi fremover blot benytte beteg-

nelsen <. For fremtiden vil vi desuden i stedet for Q* benytte betegnelsen R. Det skal understreges, at vi indtil nu kun har sikret eksistensen af de reelle tal, sådan som de fremgår af den viste konstruktion. Da der imidlertid findes konkurrerende måde at konstruere de reelle tal på, er det magtpåliggende, at disse ikke fører til et principielt andet tallegeme end vores R. Vi skal altså godtgøre, at de reelle tal i én eller anden forstand er entydigt bestemt, på nær isomorfi. Nu forholder det sig sådan, at de egenskaber der med Sætning IV.6. tillægges R ikke giver en entydig karakterisering af dem. Der skal lidt mere til. Entydighedsspørgsmålet udskydes imidlertid til senere i dette kapitel, idet vi først må skaffe det lidt mere der skal til for at opnå entydighed.

Mere om ordningen i de reelle tal

En af de vigtige egenskaber ved de reelle tals legeme er

Sætning IV.7. De reelle tals legeme er arkimedisk ordnet, dvs.

(2o) $\forall x \in R\ \exists n \in \mathbb{N}: \quad x < n.$

Bevis:

Hvis $x \leq 0$, vil $x < 1$, hvorved (2) er opfyldt. Hvis $x > 0$, findes - da Q er tæt i R - naturlige tal p og q, så at

$$x < \frac{p}{q} < x + 1.$$

Eftersom $\frac{p}{q} \leq p$ (da jo $p \leq pq$ fordi $q \geq 1$ og $p \geq 1$), vil $x < p$, hvorved (2o) er opfyldt. Q.E.D.

Vi skal nu give en omtale af øvre og nedre grænser for delmængder af de reelle tal. Først en almen definition:

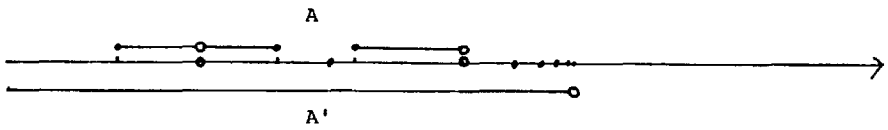
Definition: Lad M være en mængde der er ordnet ved en irrefleksiv ordningsrelation $-<$, hvis refleksive modstykke er $-\leq$. Så kaldes en delmængde A af M for opad begrænset, hvis der findes en majorant for A, dvs. et element $m \in M$, så at

$$\forall a \in A: a \mathrel{-\!\!\leq} m$$

Tilsvarende kaldes A nedad begrænset, hvis der findes en minorant for A, dvs. et element $m \in M$, så at

Hovedlinjen i beviset, der er lidt kompliceret fordi det koncentrerer en række begreber og sætninger, som normalt ses præsenteret mere opdelt - er at skaffe til den oprindelige mængde A en anden mængde A', som er mere håndterbar end A selv, og som har de samme majoranter og dermed samme øvre grænseforhold som A selv. Dernæst - og det er det, der er lidt kompliceret - bevises, at A' må være af en særlig type, nemlig bestående af samtlige reelle tal skarpt mindre end et bestemt tal.

Undervejs kommer praktisk taget alle de hidtil udvundne egenskaber ved de reele tal i spil.



$\forall\, a \in A\colon m \preceq a$.

Et element G i M kaldes øvre grænse eller supremum for mængden A, hvis G er en majorant for A, og der desuden gælder at enhver anden majorant m for A er mindst så stor som G, dvs. $G \preceq m$. Hvis - hvilket ikke behøver at være tilfældet - et eventuelt supremum for A er element i A selv, kaldes det et maksimalt element i A. Hvis G er en øvre grænse for A bruges skrivemåden $G = \sup A$.

På helt analog måde indføres begrebet nedre grænse eller infimum for en delmængde A af M. Hvis g er et sådant for A skriver vi $g = \inf A$. En nedre grænse som selv er element i A kaldes et minimalt element i A.

Det følger af antisymmetrien af den refleksive ordningsrelation, at en delmængde A højst kan have én øvre grænse (og én nedre grænse). Var nemlig G_1 og G_2 begge øvre grænser var de begge majoranter for A, hvorved $G_1 \preceq G_2$ og $G_2 \preceq G_1$, og dermed $G_1 = G_2$. Tilsvarende ræsonneres på nedre grænser.

Som antydet er det ingenlunde givet, at en delmængde i en ordnet mængde har et supremum eller et infimum. I de reelle tal forholder sagen sig således:

Sætning IV.8. Enhver ikke-tom opad begrænset delmængde af de reelle tal har en øvre grænse, og enhver ikke-tom nedad begrænset delmængde har en nedre grænse.

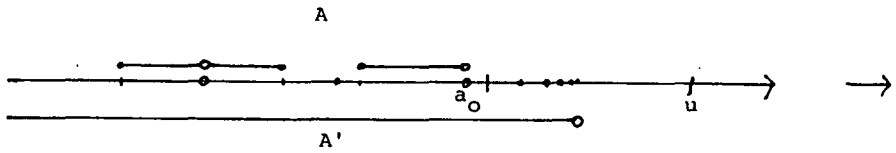
Bevis:

Lad $A \subset \mathbb{R}$ være ikke-tom og opad begrænset. Sammen med A betragtes nu mængden af de reelle tal, som hver for sig er mindre end eller lig et tal fra A:

$$A' = \{x \in \mathbb{R} \mid \exists y \in A\colon\ x \leq y\}.$$

Eftersom åbenbart $A \subseteq A'$ - thi hvis $a \in A$ findes et $y \in A$, nemlig a selv, så at $a \leq y$ - og eftersom A ikke er tom, er heller ikke A' tom. Vi vil nu indse, at A og A' har de samme majoranter.

Det er klart, at enhver majorant for A' også er majorant for den deri indeholdte mængde A (hvis m' er en majorant for A' og $a \in A$ vil $a \in A'$. hvorved $a \leq m'$). Omvendt er enhver majorant for A og-



så majorant for A'. Lad nemlig den pågældende majorant for A være m, og lad a' $\in$ A'. Så findes i følge definitionen et v i A, så at a' $\leq$ v, og da v $\leq$ m, vil også a' $\leq$ m. A og A' har altså de samme majoranter.

Vi skelner nu mellem to tilfælde, eftersom A' har et største (maksimalt) element eller ej. Hvis A' havde et sådant, G', ville det være øvre grænse for A. Thi at G' er en majorant for A følger af at G' er majorant for A'; og er dernæst m en vilkårlig majorant for A, er m også majorant for A', hvorfor, da G' tilhører A', G' $\leq$ m. Men så er G' øvre grænse for A, hvilket beviser sætningen i dette tilfælde.

Tilbage står det - langt mere omhukrævende - tilfælde, hvor A' ikke har noget største (maksimalt) element. I det følgende vil vi godtgøre, at der under denne forudsætning findes et G i R, så at

$$(21) \quad A' = \{x \in R \mid x < G\}.$$

Når dette er godtgjort, er det klart at g er øvre grænse for A. At G er en majorant for er oplagt, da i følge (21) G er en majorant for A'. Lader vi dernæst m være en vilkårlig majorant for A, er m også en majorant for A'. Så kan m åbenbart ikke tilhøre A' - vi antog jo, at A' ikke havde noget største element. Men så må m tilhøre komplementærmængden til A', og dermed må m $\geq$ G. Dette viser, at G er øvre grænse for A.

Resten af beviset består altså i at vise (21). Til den ende, der jo indebærer eksistensen af et element i R, nemlig G, er de reelle tals fuldstændighed afgørende.

Da A', som vi har set, ikke er tom, findes et element a_o i A'. Der må også findes et element u $\in$ R$\setminus$A'. Det skyldes at A' må have en majorant, f.eks. m (A' og A har jo de samme majoranter, og A har en majorant fordi A er antaget at være opad begrænset). Tallet m+1 kan så ikke tilhøre A', da ethvert a' $\in$ A' opfylder a' < m+1.

Nu vil enhver forgænger for et element i A' selv være element i A'. Lad nemlig a' $\in$ A' og lad x < a'. Da der findes et a $\in$ A, så

at $a' \leq a$, hvorved $x < a$, vil også $x \in A'$.

Vi er nu ude på for ethvert $n \in \mathbb{N}$ at bestemme et største helt tal p_n, så at $p_n 2^{-n} \in A'$ (hvorved $(p_n+1)2^{-n} \notin A'$). Derefter vil vi vise, at $(p_n 2^{-n})_n$ er en voksende fundamentalfølge. (Disse skridt kræver en række detaljer): På grund af $\mathbb{R}$'s fuldstændighed er følgen konvergent. Lad dens grænsepunkt være G. Vi vil så vise, at dette G netop kan bruges som det med (21) søgte.

For ethvert $n \in \mathbb{N}$ findes p og $q \in \mathbb{Z}$, så at

(22) (a) $p \leq a_o 2^n$, og (b) $u2^n \leq q$.

At der findes et $q \in \mathbb{Z}$, så at (22)(b) er opfyldt, følger umiddelbart af arkimediciteten af $\mathbb{R}$ (Sætning IV.7.), endda med q i $\mathbb{N}$. For at få opfyldt (22)(a) er det nok at påpege, at arkimediciteten sikrer eksistensen af et $m \in \mathbb{N}$, så at $-a_o 2^n \leq m$. Med $p = -m$ er da (22)(a) opfyldt.

Ulighederne (22) kan også udtrykkes

$$p2^{-n} \leq a_o \quad \text{og} \quad u \leq q2^{-n}.$$

Nu vil så

(23) $p2^{-n} \in A'$ og $q2^{-n} \notin A'$

(det første følger af at enhver forgænger til et A'-element selv er i A', det andet af at hvis $q2^{-n} \in A'$, ville u af samme grund tilhøre A', i strid med valget af u i $\mathbb{R} \setminus A$.)

Af (23) og af sætningen om at i $\mathbb{Z}$ har enhver opad begrænset delmængde et største element (Sætning II.3) følger, at der må findes et største helt tal, kaldet p_n, for hvilket

$$p_n 2^{-n} \in A'.$$

Tilordningen $n \sim p_n$ giver os en følge $(p_n 2^{-n})_n$. Vi vil vise, at den er en voksende fundamentalfølge.

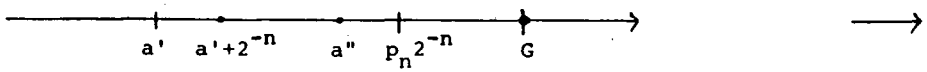
Først det voksende: hvis $n < m$ er $p_n 2^{-n} \leq p_m 2^{-m}$. Vi har, at

$$(p_n 2^{m-n})2^{-m} = p_n 2^{-n} \in A'.$$

Da $p_n 2^{m-n} \in \mathbb{Z}$ $(n < m)$ og p_m er det største hele tal, hvis produkt med 2^{-m} tilhører A', må

$$p_n 2^{m-n} \leq p_m,$$

Uligheden $2^{-n_o} \leq \frac{1}{n_o}$ fordrer egentlig et induktionsbevis. Før det! $\longrightarrow$



$\longrightarrow$

hvorved

$$p_n 2^{-n} = p_n 2^{m-n} 2^{-m} \leq p_m 2^{-m}.$$

Dernæst fundamentalfølgeegenskaben: Lad $\varepsilon \in \mathbb{R}_+$. Så findes på grund af den arkimediske ordning et $n_o \in \mathbb{N}$, for hvilket

$$n_o > \frac{1}{\varepsilon},$$

hvorved

$$2^{-n_o} \leq n_o^{-1} < \varepsilon.$$

For $m,n \in \mathbb{N}$ gælder nu, at

$$m \geq n \geq n_o \Rightarrow |p_m 2^{-m} - p_n 2^{-n}| = p_m 2^{-m} - p_n 2^{-n} <$$
$$(p_n+1)2^{-n} - p_n 2^{-n} = 2^{-n} \leq 2^{-n_o} < \varepsilon.$$

Det første lighedstegn følger af at $(p_n 2^{-n})_n$ som vist er voksende, det første ulighedstegn af, at $p_m 2^{-m} < (p_n+1)2^{-n}$. At denne ulighed gælder er en konsekvens af, at $(p_n+1)2^{-n}$ ikke kan tilhøre A', da der ellers ville være modstrid med at p_n er det største hele tal, hvis produkt med 2^{-n} tilhører A'. Når $(p_n+1)2^{-n}$ ikke kan tilhøre A' må den fremhævede ulighed gælde. Hvis den modsatte ulighed $(p_n+1)2^{-n} \leq p_m 2^{-m}$ gjaldt, ville jo $(p_n+1)2^{-n}$ være en forgænger for A'-elementer $p_m 2^{-m}$, og dermed selv et element i A'.

Da de tre næste tegn i kæden ovenfor er oplagte, har vi vist at $(p_n 2^{-n})_n$ er en fundamentalfølge. Fuldstændigheden af R sikrer derefter, at denne følge er konvergent, lad os sige med grænsepunkt G. Vi påstår nu, at (21) gælder, altså at

$$A' = \{x \in R \mid x < G\}.$$

At "$\supseteq$" gælder er lettest at indse: Lad $x < G$. Så findes, da $p_n 2^{-n} \to G$ for $n \to \infty$, et $n_1 \in \mathbb{N}$, så at

$$\forall n \in \mathbb{N}: \quad n \geq n_1 \Rightarrow x < p_n 2^{-n} \leq G$$

($\varepsilon = G-x$, og følgen kan ikke overskride G, da den er voksende). Eftersom ethvert $p_n 2^{-n} \in A'$, vil også $x \in A'$.

For at vise inklusionen "$\subseteq$" må vi sno os lidt mere: Lad $a' \in A'$. Da A' ikke har noget største element, må der findes et $a'' \in A'$, så at $a' < a''$ (hvis ikke ville jo ethvert element i A' være højst a', som da ville være største-element i A'). Da altså $a'+(a''-a') = a'' \in A'$, og da der (på grund af arkimediciteten af

Vi forlanger ikke, at legemet L er kommutativt, altså at · er kommutativ. ⟶

R) findes et $n \in \mathbb{N}$, så at $2^{-n} < a''-a'$, vil $a'+2^{-n} < a'+(a''-a') = a'' \in A'$. Altså er $a'+2^{-n}$ en forgænger for A'-elementet a", hvorfor det selv tilhører A'. Men så må videre $a' < p_n 2^{-n}$. Alternativt ville jo $a' \geq p_n 2^{-n}$, og dermed

$$(p_n+1)2^{-n} = p_n 2^{-n} + 2^{-n} \leq a' + 2^{-n} \in A',$$

i strid med definitionen af p_n. Da $(p_n 2^{-n})_n$ er voksende, vil for alle n, $p_n 2^{-n} \leq G$, og sammenholdes dette med den ovenfor opnåede ulighed $a' < p_n 2^{-n}$, slutter vi, at $a' < G$. Men det beviser inklusionen "$\subseteq$".

Hermed er sætningen bevist.

Det reelle tallegemes entydighed

For hvert af de talområder, der er behandlet i de foregående kapitler, har vi påvist deres entydighed, på nær isomorfi. Der er nu nærliggende at beskæftige sig med dette spørgsmål for de reelle tals vedkommende, ikke mindst da der er andre konstruktioner end den her valgte af de reelle tal, konstruktioner som er meget forskellige fra vores. Det viser sig, at de reelle tals legeme er entydigt bestemt, på nær isomorfi, hvis vi ud over deres fuldstændighed hæfter os ved at ordningen i dem er arkimedisk. For at kunne indse det må vi først et øjeblik studere ordnede legemer i almindelighed lidt nøjere.

Lad $(L,+,\cdot,<)$ være et ordnet legeme, hvor ω er nulelementet og e er etelementet. At legemet er ordnet betyder, at ordningsrelationen $<$ er trichotymisk og harmonerer med addition og multiplikation som i (13) og (14). Vi antager, at legemet ikke er trivielt, dvs. at det har mere end ét element. Så er $e \neq \omega$.

Der må nu gælde, at $\omega < e$. Ellers var nemlig $e < \omega$ og dermed $-e > \omega$, hvilket ville afstedkomme, at $\omega = \omega(-e) < (-e)(-e) = e^2 = e$. Men det er uforeneligt med antagelsen om, at $\omega < e$ ikke gælder.

For ethvert $n \in \mathbb{N}$ defineres ne rekursivt ved

Det vi er ude på i det følgende er at genfinde "de rationale tal" som en delmængde af L. Først leder vi efter de naturlige tal. Det sker ved at tage udgangspunkt i ételementet i L og derefter addere det til sig selv et antal gange. Derved opstår ne for n ∈ ℕ ((24)). Overgangen til de negative multipla, og dermed til de hele tal, sker ved at tage de inverse (ved addition) til de positive multipla. Det sker i (25). Vi har nu brug for at vide, at addition af ételementet til sig selv et antal gange aldrig bringer os tilbage til udgangspunktet. Dette er indholdet i (26), der bl.a. medfører at pe = ω ⇔ p = o. Grunden til at (26) gælder, er at ω < e, og at ordningen harmonerer med kompositionen, hvilket kommer i spil adskillige gange i beviset for (26). Udsagnet (26) udtrykkes ofte således: et ordnet legeme har karakteristik o.

Beviset for (27) er trælsomt, ikke fordi det er svært, men fordi det fordrer opdeling i en del undertilfælde. Hovedsagen ligger i I. De andre tilfælde reduceres hertil ved omformning. De forskellige omformninger undervejs benytter, at + er kommutativt i L (og at kompositionerne i ℕ er kommutative), men forudsætter ikke kommutativitet af · i L.

(24) oe = ω, le = e, (n+1)e = ne+e.

For p ∈ ℤ defineres dernæst

$$(25)\qquad pe = \begin{cases} pe, & \text{hvis } p \in \mathbb{N} \\ o, & \text{hvis } p = o \\ -(-p)e, & \text{hvis } -p \in \mathbb{N} \end{cases}$$

Det ses, at der altid gælder, at pe = -(-p)e for p ∈ ℤ.

Der gælder nu, at

(26) ω < pe ⇔ p ∈ N.

Bevis for "⇐". Dette foregår ved induktion.

Vi sætter M = {p ∈ ℕ | ω < pe}. Der er da klart, at 1 ∈ M, eftersom ω < e = 1e. Antages dernæst, at p ∈ M, vil der om p+1 gælde, at (p+1)e = pe+e < ω+ω = ω, så at p+1 ∈ M. Dermed har vi vist, at M = ℕ, hvorved for ethvert p ∈ ℕ: ω < pe.

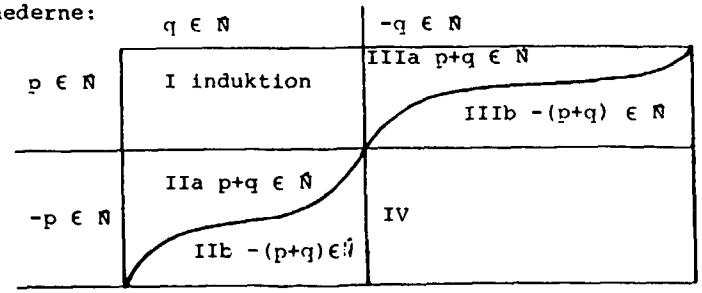
Beviset for "⇒" sker således: Hvis ω < pe, må p ≠ o, da vi har defineret oe = ω. Hvis nu p < o, måtte -p > o, dvs. -p ∈ ℕ, og dermed (i kraft af det ovenstående bevis) ω < (-p)e = -pe, så at pe < ω i strid med, at ω <pe.

Af (26) følger videre, at pe = ω ⇔ p = o.

Som man kunne forvente og håbe det, gælder at

(27) (p+q)e = pe+qe, p,q ∈ ℤ

For at bevise dette må vi dele op i en række tilfælde, hvis hovedtilfælde er illustreret af følgende skema, der ikke udtømmer mulighederne:



Først vises (27) i tilfælde I, hvor $p,q \in \mathbb{N}$. For $q \in \mathbb{N}$ defineres

$M_q = \{p \in \mathbb{N} \mid (p+q)e = pe + qe\}$.

Så vil M_q opfylde induktionsbetingelserne. Thi $1 \in M_q$, da $(1+q)e = qe + e = 1e + qe$. Hvis endvidere $p \in M_q$, har vi at

$((p+1)+q)e = ((p+q)+1)e = (p+q)e + e = pe + qe + e$

$= pe + e + qe = (p+1)e + qe$,

hvor det tredje lighedstegn følger af induktionsforudsætningen $p \in M_q$. Hermed er vist, at $p+1 \in M_q$. Så er $M_q = \mathbb{N}$.

På dette grundlag finder vi, at for $p > q$ $(p,q \in \mathbb{N})$, er $(p-q)e = pe - qe$, idet $(p-q)e + qe = ((p-q)+q)e = pe$, da $p-q \in \mathbb{N}$.

Nu kan vi behandle tilfælde IIa: $-p \in \mathbb{N}$, $q \in \mathbb{N}$, $p+q \in \mathbb{N}$. Vi har nemlig, da $q > -p$, at $(p+q)e = (q-(-p))e = qe - (-p)e$ $= qe + pe$.

På helt symmetrisk måde bevises påstanden i tilfælde IIIa (der er blot byttet om på p og q).

I tilfælde IIb går vi således frem: Vi har $-p \in \mathbb{N}$, $q \in \mathbb{N}$, $-(p+q) \in \mathbb{N}$. Derved får vi, at

$(p+q)e = (-(-p-q))e = -((-p-q)e) = -((-p) + (-q)e) =$

$-(-p)e - (-q)e = pe + qe$,

hvor det springende punkt ligger i det tredje lighedstegn, som følger af IIIa med -p i p's rolle og -q i q's.

Endnu et symmetrisk argument giver os tilfælde IIIb.

Tilfældene IIa og IIb henholdsvis IIIa og IIIb er ikke helt udtømmende for II og III. Det kan nemlig i begge situationerne forekomme, at $p+q = 0$. Men så er jo $-p = q$, og $(p+q)e = 0 = pe - pe = pe + (-p)e = pe + qe$, hvilket viser (27) i denne situation.

Hvad endelig tilfælde IV angår, finder vi at $(-p \in \mathbb{N}, -q \in \mathbb{N})$

$(p+q)e = -(-p-q)e = -((-p)e + (-q)e) = -(-p)e - (-q) = pe + qe$

hvor det andet lighedstegn er en konsekvens af I, med -p og -q i stedet for p og q.

For at have bevist (27) mangler vi blot at se på det tilfæl-

Hold øje med, at vi ikke noget sted forudsætter, at · er kommutativ i L.

Det er på dette sted at vi når til at genfinde de rationale tal som delmængde (dellegeme) af L, idet L_o består af de "formelle brøker" af "formelle hele tal" (pe-er og qe-er).

Strengt taget bør vi i øvrigt gøre rede for, at $(qe)^{-1}$ eksisterer. Det skyldes, at $qe \neq \omega$, når $q \neq o$, hvorved qe er invertibel med hensyn til · i L.

de, hvor enten $p = o$ eller $q = o$ (eller begge). Men i dette tilfælde er (27) trivielt opfyldt, fordi $oe = \omega$. Hermed er (27) bevist.

Også for multiplikation gælder det forventelige:

(28) $\quad (pq)e = (pe)(qe)$, $p,q \in \mathbb{Z}$.

Også dette bevises ved induktion.

Lad $M_q = \{p \in \mathbb{N} \mid (pq)e = (pe)(qe)\}$. Vi har nu, at $1 \in M_q$, da $(1q)e = qe = e(qe) = (1e)(qe)$. Hvis videre $p \in M_q$, vil

$((p+1)q)e = (pq+q)e = (pq)e + qe = (pe)(qe) + qe$

$= (pe + e)(qe) = ((p+1)e)(qe)$,

hvor det andet lighedstegn følger af (27), det tredje af forudsætningen $p \in M_q$. Dette viser, at $p+1 \in M_q$, så at $M_q = \mathbb{N}$. Dermed har vi indset, at $(pq)e = (pe)(qe)$ for $p \in \mathbb{N}$, $q \in \mathbb{Z}$.

Hvis $-p \in \mathbb{N}$ og $q \in \mathbb{Z}$, finder vi at

$(pq)e = ((-(-p))q)e = (-((-p)q))e = -((-p)q)e$

$= -((-p)e)(qe) = (-(-p)e)(qe) = (pe)(qe)$,

idet det fjerde lighedstegn skyldes det ovenfor beviste, med $-p \in \mathbb{N}$ og $q \in \mathbb{Z}$.

Er endelig $p = o$, vil $(pq)e = (oq)e = oe = \omega = \omega(qe) = (oe)(qe) = (pe)(qe)$, således at (28) også er bevist for $p = o$, $q \in \mathbb{Z}$. Hermed er i alt (28) bevist.

Af (28) følger i øvrigt, at $(pe)(qe) = (qe)(pe)$ for $p,q \in \mathbb{Z}$, da $pq = qp$ i $\mathbb{Z}$.

Vi går nu over til i L at betragte mængden

$$L_o = \{(pe)(qe)^{-1} \mid p \in \mathbb{Z},\ q \in \mathbb{Z} \setminus \{o\}\}.$$

Det er her klart, at ethvert element i L_o har en fremstilling af formen

$$(p'e)(q'e)^{-1} \quad \text{for et } q' \in \mathbb{N}.$$

Thi da

$$(pe)(qe)^{-1} = (pe)(qe)(qe)^{-1}(qe)^{-1} = ((pq)e)((qe)(qe))^{-1}$$
$$= ((pq)e)((qe)^2)^{-1} = ((pq)e)(q^2e)^{-1}$$

Dette resultat skal vi bruge nedenfor.

Skulle vi have overholdt de formelle spilleregler efter bogstaven, burde vi have betragtet $r \in Q$ og omtalt p/q som en repræsentant for r osv. Men den øvelse er det vist ikke længere nødvendigt at tærske langhalm på.

opnår vi det ønskede med $p' = pq$ og $q' = q^2 > o$.

Vi har derfor også, at

$$L_o = \{(pe)(qe)^{-1} \mid p \in \mathbb{Z},\ q \in \mathbb{N}\}.$$

Der gælder i øvrigt for vilkårlige $p \in \mathbb{Z}$, $q \in \mathbb{Z} \setminus \{o\}$, at $(pe)(qe)^{-1} = (qe)^{-1}(pe)$, fordi vi af $(pe) = (qe)^{-1}(qe)(pe) = (qe)^{-1}(pe)(qe)$ kan slutte dette.

Vi definerer nu afbildningen

$$\phi: Q \to L_o$$

ved

$$\phi(\frac{p}{q}) = (pe)(qe)^{-1}.$$

For at dette skal være en definition, må vi godtgøre, at værdien af ϕ er den samme, uanset hvilke ækvivalente brøker vi betragter. Dette sker på følgende måde:

$$\frac{p}{q} = \frac{p'}{q'} \Leftrightarrow pq' - p'q = o \Leftrightarrow (pq'-p'q)e = o \Leftrightarrow (pq')e = (p'q)e$$
$$\Leftrightarrow (pe)(q'e) = (p'e)(qe) \Leftrightarrow (pe)(qe)^{-1}(q'e) = p'e$$
$$\Leftrightarrow (pe)(qe)^{-1} = (p'e)(q'e)^{-1}.$$

Da der hersker biimplikation mellem den første og sidste påstand, har vi ud over, at definitionen af ϕ er tilladelig, vist, at ϕ er injektiv. At ϕ desuden er surjektiv er oplagt, da $(pe)(qe)^{-1}$ er billede af $\frac{p}{q} \in Q$.

Nu er ϕ også en homomorfi, thi

$$\phi(\frac{p}{q} + \frac{p'}{q'}) = \phi(\frac{pq' + qp'}{qq'}) = ((pq')e + (qp')e)((qq')e)^{-1} =$$
$$((pq')e)((qq')e)^{-1} + ((qp')e)((qq')e)^{-1}$$
$$= (pe)(q'e)((qe)(q'e))^{-1} + (p'e)(qe)((q'e)(qe))^{-1}$$
$$= (pe)(q'e)(q'e)^{-1}(qe)^{-1} + (p'e)(qe)(qe)^{-1}(q'e)^{-1}$$
$$= (pe)(qe)^{-1} + (p'e)(q'e)^{-1}$$
$$= \phi(\frac{p}{q}) + \phi(\frac{p'}{q'}),$$

og

At $(L_o,+,\cdot)$ er kommutativ (en konsekvens af isomorfien) følger altså, selv om $(L,+,\cdot)$ ikke er antaget at være det.

Den omvendte implikation følger selvfølgelig også af den angivne:

$\varphi(p/q) > \omega \Rightarrow p/q > o.$

Var nemlig under den anførte præmis $p/q < o$, ville $-p/q > o$, og dermed

$\omega < \varphi(-p/q) = -\varphi(p/q),$

i strid med, at $\varphi(p/q) > \omega$.

Der gælder faktisk, at ethvert arkimedisk ordnet legeme er kommutativt. Denne, måske noget overraskende, påstand vil vi afstå fra at bevise, da det følgende ikke beror på dens rigtighed.

$$\phi(\tfrac{p}{q}\,\tfrac{p'}{q'}) = ((pp')e)((qq')e)^{-1} = (pe)(p'e)(q'e)^{-1}(qe)^{-1}$$
$$= (pe)(qe)^{-1}(p'e)(q'e)^{-1}$$
$$= \phi(\tfrac{p}{q})\cdot\phi(\tfrac{p'}{q'}).$$

I alt har vi godtgjort, at ϕ er en isomorfi mellem $\mathbb{Q}$ og L_o. Specielt er $(L_o,+,\cdot)$ et kommutativt legeme, det såkaldte primlegeme.

Der gælder ydermere, at ϕ er ordenstro, dvs. at

$$\frac{p}{q} > o \Rightarrow \phi(\tfrac{p}{q}) = (pe)(qe)^{-1} > \omega .$$

Da $\frac{p}{q} > o \Leftrightarrow pq > o$, er ordenstroskaben ækvivalent med, at

$$pq > o \Rightarrow (pe)(qe)^{-1} > \omega.$$

Nu er imidlertid

$$pq > o \Leftrightarrow (pq)e > \omega \Leftrightarrow (pe)(qe) > \omega \Leftrightarrow (pe)(qe)^{-1}(qe)^2 > \omega$$
$$\Leftrightarrow (pe)(qe)^{-1} > \omega((qe)^2)^{-1} = \omega.$$

Vi benytter her, at $(qe)^2$ er invertibel, hvilket skyldes, at $(qe)^2 = q^2e > \omega$, da $q^2 > o$.

Dette viser, et ϕ er ordenstro. Således er ϕ en ordenstro isomorfi af $\mathbb{Q}$ på L_o.

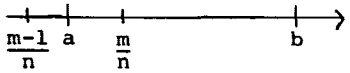
Med dette resultat in mente er der intet forgjort i at identificere L_o med $\mathbb{Q}$, således at vi kan opfatte $\mathbb{Q}$ som indlejret ordenstro isomorft som et dellegeme af $(L,+,\cdot,<)$. En sådan indlejring kan gennemføres for ethvert ordnet legeme.

Vi taler nu om et ordnet legeme $(L,+,\cdot,<)$ som arkimedisk ordnet, hvis

(29) $\quad \forall a \in L\ \exists n \in \mathbb{N}: a < n,$

hvor meningen med påstanden hentes i den nævnte indlejring, der også tillader os at opfatte $\mathbb{N}$ som en delmængde af L.

Bevisgangen er denne: Først bestemmes et $n \in \mathbb{N}$, så at $\frac{1}{n} < b-a$. Da altså 1/n er mindre end afstanden mellem a og b, bør der findes et tal af formen m/n mellem a og b. Det indses ved at vi som m vælger det mindste hele tal, for hvilket $a < \frac{m}{n}$. Da så $\frac{m-1}{n} \leq a$, er $\frac{m}{n} \leq a+\frac{1}{n} < b$.



Det gælder nu, at $(L,+,\cdot,<)$ er arkimedisk ordnet, hvis og kun hvis $Q(L_o)$ er tæt i L, dvs, hvis og kun hvis

(3o) $\quad \forall a,b \in L: [a < b \Rightarrow \exists \frac{p}{q} \in Q: a < \frac{p}{q} < b]$.

Denne ækvivalens indses på følgende måde:

Hvis (3o) er opfyldt, kan vi finde $p \in \mathbb{Z}$, $q \in \mathbb{N}$ (da ethvert element i L_o (Q) har en fremstilling med $q \in \mathbb{N}$) til $a \in L$, så at

$$a < \frac{p}{q} < a+1$$

Det er oplagt, at vi endda i uligheden $a < \frac{p}{q}$ kan opnå at benytte et $p > o$, om fornødent ved for $p < o$ at erstatte p med -p, (da i så fald $\frac{p}{q} < \frac{-p}{q}$).

Eftersom for $p,q > o$, $\frac{p}{q} \leq p$, vil vi få

$$a < \frac{p}{q} \leq p,$$

hvilket viser, at L er arkimedisk ordnet.

Lad omvendt $(L,+,\cdot,<)$ være arkimedisk ordnet, og lad $a < b$. Så vil $b-a > \omega$, og dermed $(b-a)^{-1} > \omega$. Da L er arkimedisk ordnet, findes $n \in \mathbb{N}$, så at

$$n > (b-a)^{-1},$$

hvilket er ensbetydende med, at

$$\frac{1}{n} < b-a.$$

Nu ser vi på mængden M af hele tal p, der opfylder, at $na < p$ (for de betragtede værdier af a og n). M er ikke-tom, på grund af arkimediciteten. M er endvidere nedad begrænset i $\mathbb{Z}$,f.eks. af et naturligt tal q opfyldende $-na < q$ og dermed også $-q < na < p$. Men så har, i følge Sætning II.3 M et mindste element m. Om det må der gælde at

$$(m-1) \leq na$$

Jfr. en tidligere bemærkning vil et sådant legeme automatisk være kontinuert, selv om det ikke forudsættes. Dette er også en umiddelbar konsekvens af isomorfien med R.

(ellers ville $m-1 \in M$ i strid med, at m er det mindste element i M). Heraf slutter vi, at

$$\frac{m-1}{n} \leq a,$$

og videre, at

$$\frac{m}{n} \leq a + \frac{1}{n} < a + b - a = b \text{ , altså } \frac{m}{n} < b.$$

Men da jo også $m \in M$, vil endvidere

$$na < m,$$

så at $a < \frac{m}{n}$.

Sammenholdes denne ulighed med den ovenfor opnåede, får vi

$$a < \frac{m}{n} < b,$$

hvilket viser (3o) .

*

Ved hjælp af denne afstikker til en generel situation kan vi nu få tilgodeset vor egentlige interesse i denne sag:

Sætning IV.9. De reelle tals legeme er i følgende forstand entydigt bestemt: Ethvert fuldstændigt, arkimedisk ordnet legeme er ordenstro isomorft med de reelle tals legeme.

Bevis:
Lad $(L,+,\cdot,<)$ være det omtalte fuldstændige, arkimedisk ordnede legeme. Så dannes efter opskriften ovenfor L_o som et med Q ordenstro isomorft dellegeme af L (via isomorfien ϕ). Opgaven er nu at udnytte dette til at skabe en isomorfi mellem R og L. Dette foregår således:

Det første skridt består i at indse (på basis af arkimedicíteten af L), at der til ethvert $a \in L$ findes en følge $(r_n)_n$ af elementer fra L_o, der konvergerer (i forhold til den numeriske

Det er forhåbentlig klart, at L_+ angiver mængden $\{a \in L \mid a > o\}$. →

Vær opmærksom på at den konvergens der er tale om er i L, ikke i L_o. →

Idéen i det næste er følgende: Vi har i L genfundet mængden af de rationale tal Q (i skikkelse af L_o), og har indset at ethvert element i L kan opfattes som grænseværdi (i L) for en følge af rationale tal (en følge i L_o). Men ethvert reelt tal er jo grænseværdi for en følge af rationale tal (· som de reelle tal konstrueres). Derfor kan vi til $a \in L$ knytte det reelle tal, der bestemmes af de samme (i relation til indlejringen af Q i L) konvergente følger, som bestemmer a. Dette giver os afbildningen ψ. Derefter består resten blot i at godtgøre, at ψ har de ønskede egenskaber. →

værdi i L, udspringende af ordningen) imod a: $r_n \to a$, for $n \to \infty$. At dette virkelig er muligt skyldes den tidligere viste ækvivalens mellem arkimedicitet og tæthed, som tillader os til ethvert $n \in \mathbb{N}$ at finde et $r_n \in L_o$, så at

$$a - \frac{1}{n} < r_n < a + \frac{1}{n},$$

og dermed

$$|a - r_n| < \frac{1}{n}$$

For givet $\varepsilon \in L_+$ findes nu $n_o \in \mathbb{N}$, så at $n_o > \frac{1}{\varepsilon}$, dvs. $\frac{1}{n_o} < \varepsilon$. Men så vil, når $n \geq n_o$:

$$|a - r_n| < \frac{1}{n} \leq \frac{1}{n_o} < \varepsilon,$$

hvilket viser, at den således konstruerede følge $(r_n)_n$ er konvergent med a som grænseværdi.

Nu sættes for $a \in L$

$$F_a = \{(r_n)_n \mid r_n \in L_o,\ r_n \to a\}\ .$$

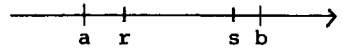
Vi har netop vist, at $F_a \neq \emptyset$ for ethvert $a \in L$. Der gælder yderligere, at enhver følge i F_a er en fundamentalfølge i L_o (Q), simpelthen fordi alle følgerne i F_a er konvergente. Af samme grund er det oplagt, at differensen mellem to følger fra F_a er en nulfølge (og dermed også en fundamentalfølge) i L_o (Q).

Dette gør det muligt for os at fremsætte følgende definition:

$$\psi(a) = \Phi_{(r_n)_n}, \text{ hvor } (r_n)_n \text{ er et vilkårligt element i } F_a.$$

Dette har mening, da $(r_n)_n$ kan opfattes som en fundamentalfølge i Q (L_o). For at der virkelig skal være tale om en definition, må $\Phi_{(r_n)_n}$ være uafhængig af valget af $(r_n)_n \in F_a$. At dette også et tilfældet følger af, at hvis $(r'_n)_n$ var et andet element i F_a, ville, i følge det ovenstående, $(r_n)_n - (r'_n)_n$ være en nulfølge, hvorved $(r_n)_n$ og $(r'_n)_n$ ville være ækvivalente i betydningen indført i begyndelsen af kapitlet, så at de vil bestemme samme klasse.

Pointen i beviset for ordenstroskaben er: Når $a < b$ $(a,b \in L)$, findes en omegn om a (med højre endepunkt $r \in \mathbb{Q}$) og en omegn om b (med venstre endepunkt $s \in \mathbb{Q}$), så at disse omegne er disjunkte. En følge der repræsenterer a må fra et vist trin at regne ligge i a-omegnen. Analogt med følger der repræsenterer b. Det fører til, at for vilkårlige to følger repræsenterende henholdsvis a $((r_n)_n)$ og b $((s_n)_n)$, må deres differens $(s_n-r_n)_n$ være større end et positivt tal, nemlig s-r, fra et vist trin. Derfor må de repræsenterede elementer $\psi(a)$ og $\psi(b)$ opfylde, at $\psi(b) > \psi(a)$.



Dermed kan vi opfatte ψ som en afbildning

$$\psi: L \rightsquigarrow R.$$

Det står nu blot tilbage at vise, at ψ er en ordenstro isomorfi.

At ψ er en homomorfi er meget let at se:

$$\psi(a+b) = \Phi_{(r_n+s_n)_n} = \Phi_{(r_n)_n+(s_n)_n} = \Phi_{(r_n)_n} + \Phi_{(s_n)_n}$$
$$= \psi(a) + \psi(b),$$

hvor det første lighedstegn følger af, at $(r_n+s_n)_n \in F_{a+b}$, når $(r_n)_n \in F_a$ og $(s_n)_n \in F_b$, og det andet af, at vi her er inden for den reelle tals legeme, som det tidligere i dette kapitel er opbygget.

På tilsvarende måde fås, at

$$\psi(ab) = \Phi_{(r_n s_n)_n} = \Phi_{(r_n)_n} \cdot \Phi_{(s_n)_n} = \psi(a)\,\psi(b).$$

Ordenstroskaben af ψ følger af:

Hvis $a,b \in L$, $a < b$, findes $r,s \in Q$ (L_o), så at $a < r < s < b$. For $(r_n)_n \in F_a$ og $(s_n)_n \in F_b$ (sådanne findes), må der eksistere trin n_1 og n_2, så at

$$r_n < r \text{ for } n \geq n_1 \text{ og } s_n > s \text{ for } n \geq n_2.$$

For $n \geq \max\{n_1,n_2\}$ vil så

$$r_n < r \text{ og } s < s_n,$$

og dermed

$$s_n - r_n > s - r \; (> o) \text{ for } n \geq n_o,$$

hvilket viser, at $(s_n-r_n)_n$ opfylder (7) . Så vil

$$\psi(b) = \Phi_{(s_n)_n} > \Phi_{(r_n)_n} = \psi(a)$$

(definitionen af >) hvilket viser ordenstroskaben.

Dette er det eneste sted hvor vi i beviset benytter fuldstændigheden af L.

Med et helt analogt bevis kan sætningen generaliseres til, at for $n \in \mathbb{N}$ og $\alpha \in R$ findes netop ét $x \in R_+$, for hvilket $x^n = \alpha$.

Af ordenstroskaben følger i øvrigt umiddelbart injektiviteten af ψ, thi hvis $\psi(a) = \psi(b)$, må $a = b$. Ellers var jo $a < b$ eller $b < a$, hvorved enten $\psi(a) < \psi(b)$ eller $\psi(b) < \psi(a)$.

Endelig surjektiviteten af ψ: Lad $\alpha \in R$, og lad $(r_n)_n$ være en fundamentalfølge fra Q repræsenterende α. Så vil $(r_n)_n$ også være en fundamentalfølge i L, thi for $\varepsilon \in L_+$ findes $\varepsilon_o \in L_o$, så at $\varepsilon_o \leq \varepsilon$ (f.eks. $\varepsilon_o = \frac{1}{k}$, hvor $k > \frac{1}{\varepsilon}$ er valgt (i N og dermed L_o) i overensstemmelse med den arkimediske ordning). Men da L var antaget at være fuldstændigt, vil $(r_n)_n$ være konvergent i L, f.eks. med grænsepunktet a. Men da er

$$\psi(a) = \Phi_{(r_n)_n} = \alpha.$$

Hermed er Sætning IV.9. bevist.

Uddragning af kvadratrødder

I indledningen til fremstillingen af de reelle tal blev behovet for deres indførelse begrundet i forskellige defekter ved de rationale tal. Den indtil nu gennemførte opbygning har taget sigte på at afhjælpe den defekt, at de rationale tal har "huller", nærmere karakteriseret ved at visse rationale talfølger som inuitivt "burde" nærme sig en grænseværdi faktisk ikke gør det inden for de rationale tals område. Derimod har vi indtil nu ikke berørt den defekt, at visse ligninger (som f.eks. $x^2 = 2$) ikke kan løses inden for de rationale tals mængde. Denne defekt afhjælpes med følgende sætning:

Sætning IV.10. Enhver ligning af formen $x^2 = \alpha$ ($\alpha \in R$, $\alpha > 0$) har én og kun én positiv løsning i de reelle tal. Denne løsning betegnes $\sqrt{\alpha}$ (kvadratroden af α).

Bevis: Entydigheden er simpel: Hvis nemlig β_1 og β_2 begge var positive reelle tal, som opfyldte

$$\beta_1^2 = \alpha \text{ og } \beta_2^2 = \alpha ,$$

var $\beta_1^2 - \beta_2^2 = 0$ og dermed $(\beta_1+\beta_2)(\beta_1-\beta_2) = 0$. Da nulreglen gælder i $(R,+,\cdot)$, må enten $\beta_1 = \beta_2$ eller $\beta_1 = -\beta_2$. Den sidste mulighed kan ikke foreligge, da $\beta_2 > 0$ medfører, at $(\beta_1 =) -\beta_2 < 0$,

Det intuitive indhold i dette skridt er at inddele et passende interval uden om $]\alpha-\varepsilon,\alpha[$ i tilstrækkeligt små delintervaller, med rationale kvadrattal som delepunkter, så at mindst ét af disse delepunkter ligger i $]\alpha-\varepsilon,\varepsilon[$.

Faktisk vil $]\alpha-\varepsilon,\varepsilon[$ også være indeholdt i intervallet $]o,k^2[$, men det er bekvemmere at se på $]o,k^2]$ af hensyn til det følgende.

Det sidste endepunkt er $k^2 = \frac{(kq)^2}{q^2}$, det næstsidste $\frac{(kq-1)^2}{q^2}$.

i strid med, at $\beta_1 > o$. Altså er $\beta_1 = \beta_2$.

Eksistensdelen af beviset baseres på følgende hovedlinje: Der konstrueres en følge $(r_n)_n$ af rationale tal, som har en grænseværdi $\beta \in \mathbb{R}$ opfyldende, at $\beta^2 = \alpha$. Nærmere bestemt foregår der følgende: en vis aftagende følge $(\varepsilon_n)_n$ af positive reelle tal dannes, så at $\varepsilon_n \to o$, for $n\to\infty$. Til hvert $n \in \mathbb{N}$ bestemmes så et $r_n \in Q$, for hvilket

$$\alpha - \varepsilon_n < r_n^2 < \alpha.$$

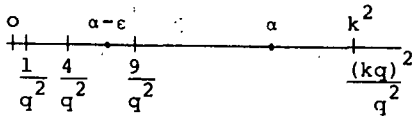
Dette giver anledning til en følge $(r_n)_n$, der ydermere kan konstrueres strengt voksende, og hvorfom det gælder, at $r_n^2 \to \alpha$ for $n \to \infty$. I konstruktionen opnås, at $(r_n)_n$ bliver en fundamentalfølge, hvorved den har en grænseværdi $\beta \in \mathbb{R}$, fordi $\mathbb{R}$ er fuldstændig. Da $r_n \to \beta$, må $r_n^2 \to \beta^2$, og dermed, da også $r_n^2 \to \alpha$, $\beta^2 = \alpha$. Endelig udføres konstruktionen sådan, at det bliver klart, at $\beta > o$.

Vi skrider nu til udførelsen af det omtalte program. Det sker i fem skridt.

Det første skridt, som er det sværeste, er at indse, at til ethvert reelt tal $\varepsilon > o$, findes naturlige tal p,q, så at

$$\alpha - \varepsilon < \frac{p^2}{q^2} < \alpha.$$

Det er åbenbart nok at betragte positive ε, hvor $\varepsilon<\alpha$ (kan konstruktionen gennemføres for ethvert sådant, kan den gennemføres for ethvert $\varepsilon>o$). Til den ende vælges nu først et $k \in \mathbb{N}$, så at $k^2 > \alpha$ (dette er muligt, fordi de reelle tal er arkimedisk ordnet). Derved vil $]\alpha-\varepsilon,\alpha[$ være indeholdt i intervallet $]o,k^2]$.



Nu vil vi finde et $q \in \mathbb{N}$, så at $]o,k^2]$ kan opdeles i disjunkte intervaller, af forskellig længde, men alle af længde mindre end ε:

$$]o,k^2] =]o,\tfrac{1^2}{q^2}]\cup]\tfrac{1^2}{q^2},\tfrac{2^2}{q^2}]\cup \ldots\cup]\tfrac{p^2}{q^2},\tfrac{(p+1)^2}{q^2}]\cup\ldots\cup]\tfrac{(kq-1)^2}{q^2},\tfrac{(kq)^2}{q^2}]$$

For et vilkårligt $q \in \mathbb{N}$ gælder (for p=o,1,2,...kq-1)

Dette er blot en kompakt skrivemåde for den lange linje på den foregående side.

Detaljerne i denne begrundelse er: Hvis både p^2/q^2 og $(p+1)^2/q^2$ falder uden for $]\alpha-\varepsilon,\varepsilon[$, må

$$\frac{p^2}{q^2} \leq \alpha-\varepsilon \text{ eller } \frac{p^2}{q^2} \geq \alpha, \quad \text{og} \quad \frac{(p+1)^2}{q^2} \leq \alpha-\varepsilon \text{ eller } \frac{(p+1)^2}{q^2} \geq \alpha .$$

Men der kan ikke være tale om, at der gælder $p^2/q^2 \geq \alpha$, da i så fald $p^2/q^2 \geq \alpha' > \alpha$, i strid med den venstre ulighed i (32). Altså må $p^2/q^2 \leq \alpha-\varepsilon$. På tilsvarende måde kan vi ikke have, at $(p+1)^2/q^2 \leq \alpha-\varepsilon$, da i så fald $(p+1)^2/q^2 \leq \alpha-\varepsilon < \alpha'$, i strid med den højre ulighed i (32).

$$\frac{(p+1)^2}{q^2} - \frac{p^2}{q^2} = \frac{2p+1}{q^2} \leq \frac{2(kq-1)+1}{q^2} = \frac{2kq-1}{q^2} < \frac{2kq}{q^2} = \frac{2k}{q}$$

Nu vælges et $q \in \mathbb{N}$, der opfylder $q > \frac{2k}{\varepsilon}$ (muligt på grund af arkimediciteten)

$$(31) \quad \frac{(p+1)^2}{q^2} - \frac{p^2}{q^2} < \varepsilon \text{ for } p = o,1,2,\ldots kq-1$$

Lad os dernæst vælge et vilkårligt element, α', i $]\alpha-\varepsilon,\alpha[$. Da

$$]\alpha-\varepsilon,\alpha[\subseteq]o,k^2] = \bigcup_{p=o}^{kq-1}]\frac{p^2}{q^2}, \frac{(p+1)^2}{q^2}]$$

findes ét (og kun ét) interval $]\frac{p^2}{q^2}, \frac{(p+1)^2}{q^2}]$ $(p = o,1,2,\ldots kq-1)$, som indeholder α':

$$(32) \quad \frac{p^2}{q^2} < \alpha' \leq \frac{(p+1)^2}{q^2} .$$

Nu må enten $\frac{p^2}{q^2}$ eller $\frac{(p+1)^2}{q^2}$ (gerne begge) tilhøre $]\alpha-\varepsilon,\alpha[$. Thi ellers ville både $\frac{p^2}{q^2} \leq \alpha-\varepsilon$ og $\frac{(p+1)^2}{q^2} \geq \alpha$, hvilket ville afstedkomme, at

$$\frac{(p+1)^2}{q^2} - \frac{p^2}{q^2} \geq \alpha - (\alpha - \varepsilon) = \varepsilon,$$

i strid med, at q er valgt, så at (31) gælder (for alle p, $p = o,1,2,\ldots kq-1$).

Hermed har vi godtgjort, at mindst ét af tallene $\frac{p^2}{q^2}$, $p = o,1\ldots kq$ tilhører $]\alpha-\varepsilon,\alpha[$:

$$\alpha - \varepsilon < \frac{p^2}{q^2} < \alpha.$$

Da $o = \frac{o}{q^2}$ og $k^2 = \frac{(kq)^2}{q^2}$ ikke tilhører $]\alpha-\varepsilon,\alpha[$, må det pågældende tal $\frac{p^2}{q^2}$ findes blandt dem, hvor $p = 1,\ldots kq-1$. Specielt må det være positivt.

Hermed er første skridt gennemført.

Andet skridt består i først at vælge $n_o \in \mathbb{N}$, så at $\frac{1}{n_o} < \alpha$ (arkimediciteten). Derefter vælges i overensstemmelse med det før-

Den benyttede fremgangsmåde forudsætter i virkeligheden en instans af rekursionssætningen fra Kapitel I. Vi vil ikke gå i detaljer hermed, da fremgangsmåden ikke skulle være logisk vanskelig. For de utrygge henvises til rekursionssætningen med $A = \mathbb{N}x]o,\alpha[$, $a = (1,r_1)$ og $g: \mathbb{N}x]o,\alpha[\sim \mathbb{N}x]o,\alpha[$, hvor g er defineret ved

$$g(m,x) = (S(m), \text{"valg"}(\min\{\frac{1}{(n_o+1)+m}, \alpha-x^2\})),$$

og hvor "valg"(ε) angiver den funktion, der til $\varepsilon > o$ ($o < \alpha$) vælger et $r \in \mathbb{Q}$ opfyldende $\alpha-\varepsilon < r^2 < \alpha$(første skridt). (Til feinschmeckerne: dette forudsætter faktisk udvalgsaksiomet). Rekursionssætningen sikrer så eksistensen af $f: \mathbb{N} \sim A$ ($=\mathbb{N}x]o,\alpha[$) (tænk på $f(n) = (n,r_n)$), opfyldende $f(S(n)) = g(f(n))$.

Læg mærke til, at

$$\varepsilon_n \leq \frac{1}{n_o+n} \text{ og } \varepsilon_n \leq \alpha-r_{n-1}^2.$$

Dette benyttes et par gange i det følgende.

Hvis $r_n \geq r_{n+1}$ ville (på grund af produktets harmoni med ordningen, og fordi $r_n > o$ og $r_{n+1} > o$):

$$r_n^2 = r_n \cdot r_n \geq r_n \cdot r_{n+1} \geq r_{n+1} \cdot r_{n+1} = r_{n+1}^2.$$

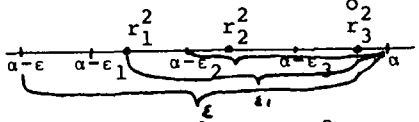
ste skridt

$$r_1 = \frac{p_1}{q_1}, \text{ så at } \alpha - \frac{1}{n_o+1} < r_1^2 < \alpha$$

Dernæst sættes $\varepsilon_2 = \min\{\frac{1}{n_o+2}, \alpha-r_1^2\}$ og vi vælger nu

$$r_2 = \frac{p_2}{q_2}, \text{ aå at } \alpha - \varepsilon_2 < r_2^2 < \alpha.$$

Videre sættes $\varepsilon_3 = \min\{\frac{1}{n_o+3}, \alpha- r_2^2\}$ og $r_3 = \frac{p_3}{q_3}$ vælges, så at $\alpha - \varepsilon_3 < r_3 < \alpha$.



Således fortsættes. Generelt sættes rekursivt

$$\varepsilon_n = \min\{\frac{1}{n_o+n}, \alpha-r_{n-1}^2\} \text{ og } r_n = \frac{p_n}{q_n} \text{ vælges i overensstemmelse med første skridt, så at}$$

$$(33)\quad \alpha - \varepsilon_n < r_n^2 < \alpha \quad , n \in \mathbb{N}.$$

Da der til ethvert $n \in \mathbb{N}$ er produceret et $r_n \in Q_+$, har vi en rational talfølge $(r_n)_n$.

Det tredje skridt består i at konstatere, at denne talfølge er strengt voksende og dens kvadrat konvergent mod α. Dette er allerede næsten klart ud fra konstruktionen:

At følgen er strengt voksende ses af, at

$$r_{n+1}^2 > \alpha - \varepsilon_{n+1} \geq \alpha-(\alpha - r_n^2) = r_n^2,$$

hvorved $r_{n+1} > r_n$.

At $r_n^2 \to \alpha$ for $n \to \infty$ følger således: For $\varepsilon > o$ vælges $M \in \mathbb{N}$ (arkimediciteten), så at

$$\frac{1}{n_o+M} < \varepsilon.$$

Så vil

$$\varepsilon_M = \min\{\frac{1}{n_o+M}, \alpha - r_{M-1}^2\} \leq \frac{1}{n_o+M} < \varepsilon$$

og dermed

$$\alpha - \varepsilon < \alpha - \varepsilon_M < r_M^2 < \alpha.$$

Lighedstegnet følger af, at $|(r_m-r_n)(r_m+r_n)| = |r_m^2-r_n^2|$, og af at $r_m+r_n > o$. Den første ulighed følger af trekantsuligheden:

$$|r_m^2-r_n^2| = |(r_m^2-\alpha)+(\alpha-r_n^2)| \leq |r_m^2-\alpha|+|r_n^2-\alpha|,$$

og af at $(r_n)_n$ er strengt voksende.

For $n \geq M$ vil så - da $(r_n)_n$ er strengt voksende -

$$\alpha-\varepsilon < r_M^2 < r_n^2 < \alpha.$$

Dette viser, at $r_n^2 \to \alpha$ for $n \to \infty$.

Det fjerde skridt består i at indse, at $(r_n)_n$ er en fundamentalfølge. Dertil benyttes vurderingen (for $m,n \in \mathbb{N}$):

$$|r_m-r_n| = \frac{|r_m^2 - r_n^2|}{r_m + r_n} \leq \frac{|r_m^2 - \alpha| + |r_n^2 - \alpha|}{r_1 + r_1} < \frac{\varepsilon_m + \varepsilon_n}{2r_1}$$

$$\leq \frac{\frac{1}{n_o+m} + \frac{1}{n_o+n}}{2r_1} \leq \frac{1}{2r_1(n_o+\min\{m,n\})}$$

hvor den anden ulighed følger af (33) og den tredje af definitionen på ε_m og ε_n.

Er nu $\varepsilon > o$ givet, vælges $K \in \mathbb{N}$, så at

$$\frac{1}{2r_1(n_o+K)} < \varepsilon.$$

Så vil, for $m,n \geq K$

$$|r_m-r_n| \leq \frac{1}{2r_1(n_o+\min\{m,n\})} \leq \frac{1}{2r_1(n_o+K)} < \varepsilon.$$

Dermed er fundamentalfølgepåstanden vist.

I det femte og sidste skridt udnyttes fuldstændigheden af $\mathbb{R}$ til at slutte, at $(r_n)_n$ har en grænseværdi $\beta \in \mathbb{R}$. Derved vil (Sætning IV.4.):

$$r_n^2 \to \beta^2.$$

Men da vi fra det tredje skridt har, at $r_n^2 \to \alpha$, har vi endelig (Sætning IV.1.), at $\beta^2 = \alpha$.

At $\beta > o$ er klart, fordi alle $r_n > o$ og $(r_n)_n$ er strengt voksende. Dermed er beviset for sætningen fuldført. Q.E.D.

Fremstilling af reelle tal ved g-adiske brøker

Hensigten med dette afsnit er at vise, at ethvert reelt tal kan fremstilles som sum af et helt tal (eller o) og en såkaldt g-adisk brøk, svarende til grundtallet g, hvor $g \in \mathbb{N}$, $g > 1$. Et specialtilfælde heraf fremkommer når $g = 10$, hvor vi ikke taler om 10-adiske brøker, men om decimalbrøker.

Vi lægger ud med at betragte et vilkårligt reelt tal α. Ved den hele del af α, $[\alpha]$, forstås det største hele tal mindre end eller lig med :

$$[\alpha] = \max\{h \in \mathbb{Z} \mid h \leq \alpha\}.$$

Eksistensen af $[\alpha]$ følger af, at mængden $\{h \in \mathbb{Z} \mid h \leq \alpha\}$ af hele tal er opad begrænset (Sætning II.3.). Der må øjensynlig gælde, at $[\alpha] \leq \alpha$, $\alpha < [\alpha] + 1$, så at vi i alt får

$$0 \leq \alpha - [\alpha] < 1.$$

Betragter vi nu den første rest $\alpha - [\alpha] = \alpha - a_0$ (idet vi for bekvemmelighedens skyld i det følgende sætter $a_0 = [\alpha]$), efter at vi fra α har fjernet $[\alpha]$, er der selvfølgelig ingen fornuft i at spørge hvad den hele del af denne rest er, den er jo 0. Vi kan derimod spørge hvor mange g'te-dele der er i den, eller - hvad der kommer ud på det samme - hvor mange hele der er i g gange resten. Kalder vi resten $\alpha - a_0$ for R_1, angiver altså

$$a_1 = [gR_1]$$

antallet af g'te-dele i resten $\alpha - a_0$.

Det der nu er tilbage af α er

$$\alpha - a_0 - \frac{a}{g}1,$$

hvor der selvfølgelig vil være ufornuft i at spørge om antallet af g'te-dele heri, al den stund tallet ligger i intervallet $[0, \frac{1}{g}[$. I stedet spørger vi om antallet af g^2'te-dele, lig antallet af g'te-dele i $R_2 = g(\alpha - a_0 - \frac{a}{g}1)$, lig antallet af hele (enere) i $gR_2 = g^2\alpha - g^2a_0 - ga_1$, dvs.

$$a_2 = [gR_2] = [g^2\alpha - g^2a_0 - ga_1].$$

På denne måde fortsættes, således at følgende skema opstår. Det

Læg mærke til at alene a_o <u>ikke nødvendigvis opfylder denne ulighed</u>! →

Da det er første gang vi i den formelle del af denne tekst bruger Σ-tegnet, burde det introduceres behørigt, ved at vi for $k,m \in \mathbb{Z}$, $k \leq m$, definerer (x-erne er f.eks. reelle tal)

$$\sum_{i=k}^{m} x_i = \begin{cases} x_k, \text{ hvis } k=m \\ \sum_{i=k}^{m-1} x_i + x_k, \text{ hvis } k < m \end{cases}$$

altså en rekursiv definition, der egentlig kræver rekursionssætningen fra Kapitel I.

skal bemærkes, at den generelle mekanik i skemaet først opstår fra og med 1. række:

n	R_n	a_n	rest
o		$a_o = [\alpha]$	$\alpha - a_o$
1	$R_1 = \alpha - a_o$	$a_1 = [g(\alpha - a_o)]$	$\alpha - a_o - \frac{a_1}{g}$
2	$R_2 = g\alpha - ga_o - a_1$	$a_2 = [g(g\alpha - ga_o - a_1)]$	$\alpha - a_o - \frac{a_1}{g} - \frac{a_2}{g^2}$
3	$R_3 = g^2\alpha - g^2a_o - ga_1 - a_2$	$a_3 = [g(g^2\alpha - ga_o - ga_1 - a_2)]$	$\alpha - a_o - \frac{a_1}{g} - \frac{a_2}{g^2} - \frac{a_3}{g^3}$
.			
.			
.			
n+1	$R_{n+1} = gR_n - a_n$	$a_{n+1} = [gR_{n+1}]$	$\alpha - \sum_{i=o}^{n+1} \frac{1}{g^i} a_i$
.			
.			

Systemet er altså reguleret af ligningerne

(34) $R_{n+1} = gR_n - a_n$, $n \geq 1$

og

(35) $a_n = [gR_n]$, $n \geq 1$ $a_o = [\alpha]$.

Heraf ser vi, at

$R_{n+1} = gR_n - [gR_n]$, $n \geq 1$,

således at

(36) $o \leq R_n < 1$, $n \geq 1$.

Sammenholdes dette med (35), finder vi, at

(37) $o \leq a_n < g$, $n \geq 1$.

Som eksplicitte udtryk for R_n og a_n får vi derefter

(38) $R_n = g^{n-1}\alpha - \sum_{i=o}^{n-1} g^{n-1-i} a_i$, $n \geq 1$

og heraf videre (ud fra (35))

(39) $a_n = [g^n\alpha - \sum_{i=o}^{n-1} g^{n-i} a_i]$, $n \geq 1$.

Af udtrykket (38) for R_{n+1} fås, da $o \leq R_{n+1} < 1$, $n \geq o$, ved division med g^n:

$$o \leq \alpha - \sum_{i=o}^{n} g^{-i} a_i < g^{-n},$$

og heraf, at

Der gælder nemlig (hvilket ses ved induktion), at $g^n > n$ for $n \geq o$. Da den arkimediske ordning i $\mathbb{R}$ bevirker, at der findes et $n_o \in \mathbb{N}$, så at $n_o > 1/\varepsilon$, vil for $n \geq n_o$:

$$g^n > n \geq n_o > 1/\varepsilon ,$$

og dermed $\varepsilon > g^{-n}$.

an skal tænke på udsagnet $\alpha = \sum_{i=o}^{\infty} a_i g^{-i}$ som en suggestiv skrivemåde, der blot betyder:

$$s_n \to \alpha,$$

(pr. definition).

Man kan vise - men det vil vi ikke gå nærmere ind på her - at de rationale tal netop er dem der har en periodisk g-adisk brøkfremstilling, hvor periodisk betyder, at fra et vist trin kommer cifrene (som vi lidt utraditionelt kalder g-cimalerne) i en uendeligt gentaget blok:

$$r = a_o,a_1\cdots a_k\ \underbrace{a_{k+1}\cdots a_m}_{l}\underbrace{a_{k+1}\cdots a_m}_{k}\underbrace{a_{k+1}\cdots a_m}_{k+l}\cdots\cdots$$

Der ligger egentlig lidt simpel analyse i dette. I kraft af kvotientrækkeformlen har vi nemlig

$$t_p = \sum_{i=n+1}^{p}(g-1)g^{-i} = (g-1)\sum_{i=n+1}^{p} g^{-i} = (g-1)\,\frac{1-g^{-(p-n)}}{1-g^{-1}}\,g^{-(n+1)},$$

hvoraf, da $g^{-(p-n)} \to o$ for $p \to \infty$,

$$t_p \to (g-1)\frac{g^{-(n+1)}}{1-g^{-1}} \quad \text{for } p \to \infty.$$

$$o \leq |\alpha - \sum_{i=o}^{n} a_i g^{-i}| < g^{-n}.$$

Dette viser, at følgen $(s_n)_n$, bestemt ved

$$s_n = \sum_{i=o}^{n} a_i g^{-i} \ , \ n \geq o$$

konvergerer mod α. Thi for et givet $\varepsilon > o$ vælges blot n_o, så at $g^{-n} < \varepsilon$ for $n \geq n_o$, hvilket er muligt på grund af arkimediciteten af $\mathbb{R}$.

Men så vil i alt α være fremstillet som en sum af en uendelig række med rationale led $a_i g^{-i}$, hvor $o \leq a_i < g$, for $i \geq 1$, og hvor $a_i \in \mathbb{N} \cup \{o\}$:

$$\alpha = \sum_{i=o}^{\infty} a_i g^{-i}.$$

Vi benytter skrivemåden

$$\alpha = a_o,a_1a_2a_3\cdots \quad (a_o \text{ ligger ikke nødvendigvis i } [o,g[!)$$

og siger, at α er fremstillet som en uendelig g-adisk brøk.

Hvis i den g-adiske brøkfremstilling $a_i = o$ for alle i fra et vist trin, siges den g-adiske brøk at være endelig. Hvis et tal α har en sådan fremstilling, dvs. har formen

$$\alpha = a_o + \frac{a_1}{g} + \frac{a_2}{g^2} + \ldots + \frac{a_n}{g^n}$$

for et eller andet n, er det åbenbart rationalt. Det omvendte behøver ikke at være tilfældet (se f.eks. på decimalbrøksfremstillingen af $\frac{1}{3}$).

Hvis et rationalt tal r er fremstillet som en endelig g-adisk brøk, kan det også fremstilles som en 'ægte' uendelig, hvor alle cifre er positive fra et vist trin. Det sidste led $a_n g^{-n}$, $a_n \neq o$, i den endelige g-adiske fremstilling kan nemlig skrives

$$a_n g^{-n} = (a_n - 1)g^{-n} + \sum_{i=n+1}^{\infty}(g-1)g^{-i},$$

eftersom vi har

$$\sum_{i=n+1}^{\infty}(g-1)g^{-i} = (g-1)\frac{1/g^{n+1}}{1-1/g} = (g-1)\,\frac{g}{g-1}\cdot\frac{1}{g^{n+1}} = g^{-n}.$$

Heraf følger, at hvis $r = a_o,a_1a_2\ldots a_n$ er også $r = a_o,a_1a_2\ldots a_{n-1}(a_n-1)(g-1)(g-1)\ldots$ en g-adisk brøk-fremstilling af r.

Hvis et tal har en g-adisk brøkfremstilling af den først ind-

Som eksempel i decimalbrøk har vi, at 2,1299.... er lig 2.13oo....

For $i < k$, er jo $b_k = a_k$.

førte type (altså ikke den for rationale tal med endelig fremstilling opnåede, med bare g-1'er fra et vist trin), må uendelig mange g-cimaler a_i opfylde, at $a_i < g-1$. Ellers ville nemlig α have formen

$$\alpha = \sum_{i=o}^{k} a_i g^{-i} + \sum_{i=k+1}^{\infty} (g-1)g^{-i} \quad \left(= \sum_{i=o}^{k} a_i g^{-i} + g^{-k} \right)$$

for et eller andet $k \geq o$.

Men så ville

$$\alpha - \sum_{i=o}^{k} a_i g^{-i} = g^{-k},$$

og dermed

$$\alpha g^k - \sum_{i=o}^{k} a_i g^{k-i} = 1$$

i strid med (38) (og med (36)).

Derved har vi for visse tal (nemlig de rationale tal, der har en endelig g-adisk brøkfremstilling), to mulige fremgangsmåder til at producere en uendelig g-adisk brøkfremstilling, dels den almene (den første), der sikrer at uendelig mange g-cimaler er < g-1, dels den der produceres ud fra den endelige, og hvori alle g-cimaler fra et vist trin bliver g-1. Dette viser, at g-adisk brøkfremstilling i almindelighed ikke er en entydig afføre.

Der er imidlertid entydighed, hvis man forlanger, at uendelig mange g-cimaler skal være <g-1, eller udtrykt ækvivalent: Hvis to g-adiske fremstillinger med uendelig mange g-cimaler < g-1 er forskellige, dvs. på mindst én plads udviser forskellige g-cimaler, fremstiller de forskellige reelle tal. Dette godtgøres således:

Lad $\alpha = \sum_{i=o}^{\infty} a_i g^{-i}$ og $\beta = \sum_{i=o}^{\infty} b_i g^{-i}$,

hvor ikke alle a_i-er og b_i-er er identiske. Lad k være det første nummer for hvilket $a_k \neq b_k$, f.eks. $a_k < b_k$. Så vil

$$\beta - \alpha = (b_k - a_k)g^{-k} + \sum_{i=k+1}^{\infty} (b_i - a_i)g^{-i}.$$

Da $a_i \leq g-1$ og $b_i \leq g-1$ for alle i, må $b_i - a_i \geq -(g-1)$. Der må nu findes mindst ét $i' > k$, så at $b_{i'} - a_{i'} > -(g-1)$. Ellers ville jo $b_i - a_i = -(g-1)$ for alle $i > k$, og dermed (da for

$i > k$: $o \leq b_i = a_i - (g-1) \leq o)$ $b_i = o$ for alle $i > k$, og $a_i = (g-1)$ for alle $i > k$, i strid med at uendelig mange a_i er $< g-1$.

Af det fundne følger nu:

$$\alpha - \beta = (b_k - a_k)g^{-k} + \sum_{\substack{i=k+1 \\ i \neq i'}}^{\infty} (b_i - a_i)g^{-i} + (b_{i'} - a_{i'})g^{-i'}$$

$$> (b_k - a_k)g^{-k} - (g-1) \sum_{\substack{i=k+1 \\ i \neq i'}}^{\infty} g^{-i} - (g-1)g^{-i'}$$

$$= (b_k - a_k)g^{-k} - (g-1) \sum_{i=k+1}^{\infty} g^{-i} = (b_k - a_k)g^{-k} - (g-1) \frac{g^{-k-1}}{1-1/g}$$

$$= (b_k - a_k)g^{-k} - g^{-k} = (b_k - a_k - 1)g^{-k} \geq o,$$

da $b_k - a_k > o$ og dermed $b_k - a_k \geq 1$. Alt i alt må så $\beta > \alpha$, hvilket beviser, at $\alpha \neq \beta$.

Vore betragtninger har forsynet os med beviset for følgende sætning:

<u>Sætning IV.11</u>. Lad g være et vilkårligt element i $\mathbb{N}$, $g > 1$.For ethvert reelt tal α findes et helt tal $a_o \in \mathbb{Z}$, samt tal $a_1, a_2, \ldots$, hvor $a_i \in \mathbb{N} \cup \{o\}$, $o \leq a_i \leq g-1$, for $i \geq 1$, så:

(40) $\alpha = a_o, a_1 a_2 \ldots = \sum_{i=o}^{\infty} a_i g^{-i}$.

Der findes én og kun én fremstilling af denne form, som opfylder at uendelig mange a_i er $< g-1$. Hvis en g-adisk brøk er endelig, dvs. hvis alle $a_i = o$ fra et vist trin, er det fremstillede tal rationalt. I denne situation findes der desuden en uendelig g-adisk brøk, således at alle g-cimalerne er lig g-1 fra et vist trin. Omvendt er et sådant tal, med en fremstilling indeholdende lutter g-1'er fra et vist trin, rationalt.

Der kan være grund til at henlede opmærksomheden på det specialtilfælde, hvor $g = 2$, hvor ethvert reelt tal kan fremstilles med lutter o'er og 1'er efter kommaet. Dette resultat får vi brug for i kapitlets sidste afsnit om kardinaliteten af $\mathbb{R}$.

Vi vender tilbage til den generelle situation. I den fremstilling vi opnåede i (40) er tallet før kommaet, a_o, jo ikke nødvendigvis beliggende mellem (og inclusive) o og g-1. Udnyttes imidlertid positionsfremstillingen af de naturlige tal (Sætning II.6.) kan vi ved at skrive a_o på formen $c_n c_{n-1} \cdots c_o$, hvis a_o er et naturligt tal, som o, hvis $a_o = o$, og som $-c_n c_{n-1} \cdots c_o$, hvis a_o er et negativt helt tal, opnå at fremstille det vilkårlige reelle tal α på kombineret positions- og g-adisk form med g som grundtal:

$$\alpha = \pm\, c_n c_{n-1} \cdots c_o, a_1 a_2 \cdots,$$

hvor alle c_n'er og a_i'er er større end eller lig o og mindre end eller lig g-1, og hvor $c_n > o$.

Vi skylder at undersøge om enhver følge af tal $a_1, a_2, \ldots$ fra $\mathbb{N} \cup \{o\}$, $o \leq a_i \leq g-1$, giver anledning til en uendelig gecimalbrøk $o, a_1 a_2 \ldots$ for et eller andet reelt tal. At dette er tilfældet - hvad det er - kommer ud på at den uendelige række $\sum_1^\infty a_i g^{-i}$ er konvergent, altså om afsnitsfølgen $(s_n)_n$, hvor vi har $s_n = \sum_1^n a_i g^{-i}$, har en grænseværdi i $\mathbb{R}$. Men det har den. Den er nemlig en fundamentalfølge, hvilket indses således:

For $n > m$ er, da alle led $a_i g^{-i}$ er ikke-negative, og a_i højst g-1:

$$|s_n - s_m| = \sum_1^n a_i g^{-i} - \sum_1^m a_i g^{-i} = \sum_{m+1}^n a_i g^{-i} \leq \sum_{m+1}^n (g-1) g^{-i}$$

$$= (g-1) \sum_{m+1}^n g^{-i} = (g-1) g^{-(m+1)} \frac{1-g^{-(n-m)}}{1-1/g}$$

$$= g^{-m}(1-g^{-(n-m)}) = g^{-m} - g^{-n} < g^{-m}.$$

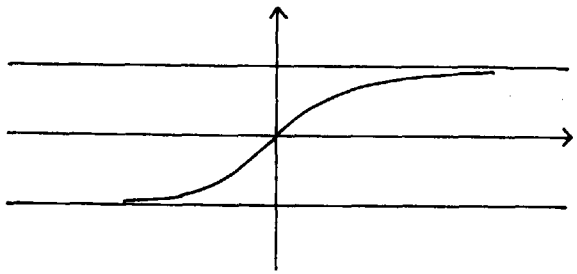
Er derefter $\varepsilon > o$ givet finder vi blot $n_o \in \mathbb{N}$, så at $g^{-n_o} < \varepsilon$. Så vil, for $n > m \geq n_o$:

$$|s_n - s_m| < g^{-m} \leq g^{-n_o} < \varepsilon,$$

hvorved fundamentalfølgeegenskaben er bevist.

Altså vil <u>enhver følge $a_o, a_1, a_2 \ldots$ ved $a_o, a_1 a_2 \ldots$ fremstille et reelt tal som undelig g-adisk brøk</u>, hvis alle a_i, $i \in \mathbb{N}$ opfylder, at $o \leq a_i \leq g-1$ (og $a_i \in \mathbb{N}$).

Der er en lang række funktioner som kunne benyttes til vort formål. Her lægger vi ud med først at angive en bijektiv afbildning $f: \mathbb{R} \sim]-1,1[$. Den har ca. grafen



Derefter transformeres $]-1,1[$ til $]a,b[$ gennem den "lineære" og bijektive afbildning $t:]-1,1[\sim]a,b[$, defineret ved

$$t(y) = \frac{b-a}{2}\, y + \frac{b+a}{2}\,.$$

(Check selv at t er en sådan afbildning.) Afbildningen $f_{a,b}$ bestemt ved $f_{a,b} = t \circ f$, vil da afbilde $]-1,1[$ bijektivt på $]a,b[$.

De reelle tals kardinalitet

I de foregående kapitler blev det godtgjort, at de deri behandlede talområder $\mathbb{N}$, $\mathbb{Z}$ og $\mathbb{Q}$ er indbyrdes ækvipotente, og dermed alle numerable. Vi skal nu undersøge ækvipotensforholdene for de reelle tals mængde i relation til de foregående talområder. Det viser sig nu, at $\mathbb{R}$ ikke er numerabel. Dette er ér af punkterne i

Sætning IV.12. (a) $\mathbb{R}$ er ækvipotent med ethvert interval $]a,b[= \{x \in \mathbb{R} \mid a < x < b\}$, hvor $a < b$.
(b) $\mathbb{R}$ er ikke numerabel.
(c) $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$ er ækvipotent med $\mathbb{R}$.

Bevis: Vi behandler (a) først. Vi lægger ud med at definere en funktion $f: \mathbb{R} \sim \mathbb{R}$, ved

$$f(x) = \frac{x}{|x|+1}\,,\quad x \in \mathbb{R}.$$

Da gælder øjensynlig, at $f(x) > 0$ for $x \in \mathbb{R}_+$ og $f(x) < 0$ for $x \in \mathbb{R}_-$. Videre har vi, at

$$-1 = \frac{-|x|-1}{|x|+1} < \frac{-|x|}{|x|+1} \le \frac{x}{|x|+1} \le \frac{|x|}{|x|+1} < \frac{|x|+1}{|x|+1} = 1.$$

Det viser, at $f(\mathbb{R}) \subseteq]-1,1[$. Imidlertid er ethvert $y \in]-1,1[$ billede ved f af et reelt tal. Thi er $y = 0$ er $y = f(0)$. Er $y > 0$ er $x = \frac{y}{1-y} > 0$ og

$$f(x) = \frac{x}{x+1} = \frac{y/1-y}{y/(1-y)+1} = y.$$

Tilsvarende er $y < 0$ billede ved f af $x = \frac{y}{1+y}$ (< 0)

I alt er $f: \mathbb{R} \sim]-1,1[$ surjektiv. Men den er også injektiv. Thi er $u \neq v$, må $f(u) \neq f(v)$. Dette er i hvert fald sandt, hvis u og v har modsat fortegn, eller én af dem er 0. Lad dernæst u og v begge være negative. Var $f(u) = f(v)$ ville

$$\frac{u}{-u+1} = f(u) = f(v) = \frac{v}{-v+1},$$

hvorved $u(-v+1) = v(-u+1)$, eller m.a.o. $-uv+u = -vu+v$, så at $u = v$. På helt analog måde argumenterer vi, hvis u og v begge er positive.

Vi har nu vist, at f er bijektiv, altså at $]-1,1[$ er ækvipotent med $\mathbb{R}$. For det vilkårlige interval $]a,b[, a < b$ definerer

Det angivne udtryk for $f_{a,b}$ svarer netop til fremstillingen af tof, jfr. side 229.

Mere præcist er der tale om $f_{o,1}$ snarere end f.

Grunden til at vi har brug for at se på intervallet [o,1] frem for intervallet]o,1[er at den konstruktion der bringes nedenfor ellers kunne give o eller 1 som resultat.

Surjektiviteten af q skyldes at p's værdimængde er]o,1[, mens q(1) = o og q(2) = 1. Injektiviteten skyldes, at q(n) = q(m) og m,n $\geq$ 3 medfører, at p(n-2) = p(m-2), og da p er bijektiv må m = n. Hvis m,n $\in$ {1,2} kan q(n) og q(m) kun være ens, hvis n = m.

Navnet diagonalargumentet kommer af, at a_n fremkommer ved at danne diagonalfølgen, dvs. følgen hvis n'te element er den n'te element fra det n'te følgeelement, altsammen efter kommaet, og derefter udskifte hvert element med dets "modsatte".

o,oooo...
o,1111...
o,olo...
o,lol...
...

vi $f_{a,b}$: $\mathbb{R} \sim]a,b[$ ved

$$f_{a,b}(x) = \frac{(b-a)}{2} \cdot \frac{x}{|x|+1} + \frac{b+a}{2}, \quad x \in \mathbb{R}.$$

En enkel efterprøvning viser, at $f_{a,b}$ afbilder $\mathbb{R}$ bijektivt på]a,b[. Dette overlades til læseren.

Hermed er (a) bevist.

Beviset for (b) beror på Cantor's berømte diagonalargument. Udgangspunktet er, at vi kan nøjes med er vise, at intervallet]o,1[ikke er ækvipotent med $\mathbb{N}$. Var det nemlig det, f.eks. gennem funktionen g: $]o,1[\sim \mathbb{N}$ (bijektiv), ville også $\mathbb{R}$ være ækvipotent med]o,1[gennem afbildningen gof, hvor f er hentet fra (a). For at vise, at]o,1[ikke er ækvipotent med $\mathbb{N}$ udnytter vi at ethvert tal i dette interval har en 2-adisk brøk-fremstilling, dvs. en fremstilling på formen $o,a_1a_2a_3\ldots$, hvor hvert a_1 er o eller 1, (Sætning IV.11.)

Antager vi nu, at]o,1[var ækvipotent med $\mathbb{N}$, f.eks. gennem afbildningen p: $\mathbb{N} \sim]o,1[$ ville også [o,1] være ækvipotent med $\mathbb{N}$. Afbildningen q: $\mathbb{N} \sim [o,1]$ defineret ved

$$q(n) = \begin{cases} o & \text{hvis } n = 1 \\ 1 & \text{hvis } n = 2 \\ p(n-2) & \text{hvis } n \geq 3 \end{cases}$$

er jo tydeligvis bijektiv. Ved hjælp af q er vi i stand til at opskrive elementerne i [o,1] i rækkefølge; den kunne f.eks. se således ud:

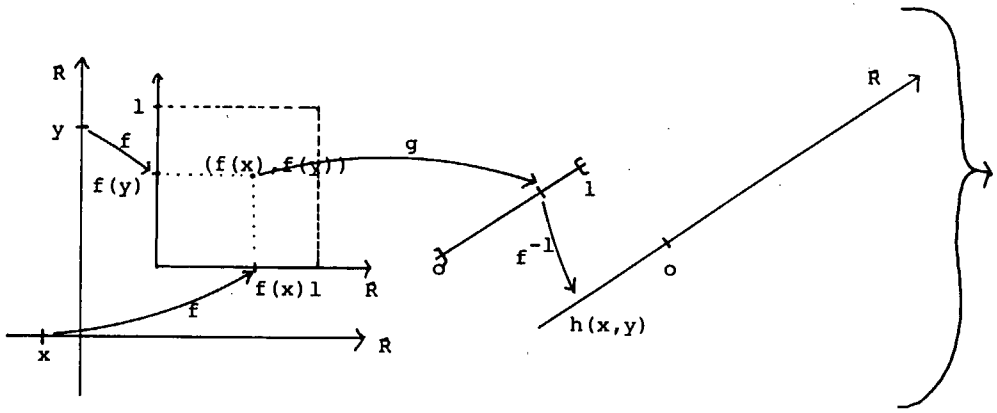
q(1) = o,ooo...
q(2) = o,lll...
q(3) = o,olo...
q(4) = o,lol...

Vi kan imidlertid angive et tal i [o,1] som ikke kan være med i rækken. Sætter vi nemlig

$$a_n = \begin{cases} o, & \text{hvis q(n) har 1 på den n'te plads efter kommaet} \\ 1, & \text{hvis q(n) har o på den n'te plads efter kommaet} \end{cases}$$

vil tallet med den 2-adiske brøkfremstilling $o,a_1a_2a_3\ldots$ ligge i [o,1].

Dette tal kan ikke være med i rækken, eller anderledes sagt,



Er f.eks. x = o,1o1ooo11o... er x_1 = 1, x_2 = o1, x_3 = ooo1, x_4 = 1,... ⟶

være billede ved q af et s ∈ ℕ. Var det nemlig det, måtte jo tallet have de samme cifre efter kommaet som q(s). Men på den s'te plads har o,a_1a_2... cifret a_s, mens q(s) har det "modsatte" ciffer, pr. definition af a_s. Dermed er (b) bevist.

Vi mangler (c): Kan vi bevise, at mængden]o,1[x]o,1[er ækvipotent med]o,1[får vi let, at ℝxℝ er ækvipotent med ℝ. Er nemlig g:]o,1[x]o,1[~]o,1[bijektiv, gælder det samme afbildningen h: ℝxℝ ~ ℝ, bestemt ved

$$h(x,y) = f^{-1}(g(f(x),f(y))),$$

hvor f er en bijektiv afbildning mellem ℝ og]o,1[, som eksisterer i følge (a).

For at vise, at]o,1[x]o,1[er ækvipotent med]o,1[betragter vi et vilkårligt (x,y) ∈]o,1[x]o,1[. De to tal x og y har hver sin entydigt bestemte 2-adiske brøk-fremstilling, der ikke ender med lutter o-er. Disse fremstillinger kan vi nu notere på en særlig måde: x = o,x_1x_2..., hvor x_1 betegner hele sættet af cifre efter kommaet til og med det første 1-tal, x_2 det næste sæt af cifre til og med det næste 1-tal osv. Det betyder at i hvert sæt x_i er alle cifre lig o på nær det sidste, som er 1. På tilsvarende måde noteres y = o,y_1y_2... Danner vi nu tallet z ved at sætte z = o,$x_1y_1x_2y_2$... hvor x_i-erne og y_i-erne stadig er de omtalte sæt af cifre, har vi fastlagt en afbildning k:]o,1[x]o,1[~]o,1[. Denne afbildning er surjektiv. Thi foretages for det vilkårlige tal z i]o,1[denne opdeling i sæt ud fra en 2-adisk brøkfremstilling som ikke ender på lutter o'er, og dannes dernæst x ved at opskrive sættene med ulige numre i rækkefølge efter kommaet, og y ved at opskrive de ligenumrede sæt, er k(x,y) = z. Afbildningen er også injektiv, thi hvis (x,y) og (x',y') er forskellige, må enten x og x' eller y og y' have mindst ét sæt forskelligt. Det bevirker, at k(x,y) og k(x',y') har forskellige fremstillinger i sæt, og dermed også i 2-adiske brøker. Men da fremstillingen i 2-adiske brøk er entydig, når denne ikke ender på lutter o'er, er k(x,y) og k(x',y') forskellige. Dermed er (c) og sætningen bevist.

V. DE KOMPLEKSE TAL

Udvidelsen af de reelle tal til de komplekse tal

Historisk indledning

Oprindelsen til de komplekse tal ligger i nogle italienske renæssancematematikeres arbejde med at løse 2. og 3. gradsligninger. Det havde længe været kendt, at mange 2. gradsligninger, f.eks. $x^2+1 = o$, ingen løsning havde. Cardano (15ol-76) gav i sin Ars Magna (1545) følgende eksempel: opgaven at dele lo i to dele, hvis produkt er 4o, er uløselig. Den kommer jo ud på at løse ligningen $x(lo-x) = 4o$, der ikke har reelle rødder. Han angiver imidlertid "sofistiske" løsninger for den, nemlig $5\pm\sqrt{-15}$.

Selv om vi med bagklogskabens privilegium kan sige at indførelsen af de komplekse tal gør det muligt at løse den slags umulige 2. gradsopgaver, som de blev kaldt, er det næppe historisk berettiget at se sporen til de komplekse tals indførelse heri; der findes jo så mange umulige opgaver i verden, som det ville være halsløs gerning at forsøge at løse. Problemet med disse 2. gradsopgaver er ikke først og fremmest at man står uden løsningsmetoder til at finde en løsning, men at der slet ingen fornuftige løsninger findes i et fornuftigt talområde (de reelle tal). Bombelli (1526-72) siger det sådan (1572): "Der er imidlertid ingen mangel ved løsningsmetoden, men ved problemet selv, der handler om det umulige, eller ikke er rigtigt stillet". Imidlertid betragtede man (dvs. folk som Tartaglia (1499-1557), Cardano og Bombelli) faktisk problemer, der både har en fornuftig løsning, og hvortil der findes en almindelig løsningsmetode, men hvor denne forløber gennem stadier, der kan give ufortolkelige resultater. Sådanne problemer finder man i sammenhæng med 3. gradsligninger. For tredjegradsligningen $x^3 = px + q$ havde (har) man løsningsformlen, den såkaldte Cardano's formel (som vistnok rettelig skyldes Tartaglia):

$$x = \sqrt[3]{q/2 + \sqrt{r}} + \sqrt[3]{q/2 - \sqrt{r}},$$

hvor $r = (q/2)^2 - (p/3)^3$. Man kan ved efterprøvning uden større vanskeligheder indse, at dette udtryk for x faktisk løser ligningen. Imidlertid giver dette jo kun mening, hvis $r \geq o$. Ser vi nu på ligningen $x^3 = 15x + 4$, som Bombelli gjorde der, konstaterer vi at $r = -121$, hvorfor løsningsmetoden ikke kan bringes i anvendelse her. På den anden side har ligningen øjensynlig den helt fredsommelige løsning $x = 4$. Men så burde løsningsmetoden jo kunne frembringe 4 som resultat:

$$4 = \sqrt[3]{2 + \sqrt{r}} + \sqrt[3]{2 - \sqrt{r}}.$$

Det ville den også kunne, hvis vi undervejs i regningerne opererede med $\sqrt{-121}$ formelt, som om ingen ting var hændt! Og det skridt tog de omtalte italienere faktisk. Bombelli giver i sin fremstilling regneregler for $\sqrt{-1}$ (det vi i dag kalder den imaginære enhed og betegner i), i følge hvilke $\sqrt{-121} = 11\sqrt{-1}$. Herigennem når han frem til, at

$$\sqrt[3]{2 + \sqrt{-121}} = 2 + \sqrt{-1} \text{ og } \sqrt[3]{2 - \sqrt{-121}} = 2 - \sqrt{-1}$$

(check selv), der netop har summen 4.

Fristelsen til at foretage formelle, men i forhold til da gældende regler ulovlige, manipulationer som middel til at skaffe lovlige resultater kan i mangt og meget sidestilles med de tidligere omtalte fristelser til at operere med negative og med irrationale tal. Skønt "ikke-eksisterende" og vanskeligt fortolkelige leverer de et slagkraftigt hjælpemiddel, som gennem tilvænning bliver velbekendt og selvstændiggjort, men som først langt senere gøres til genstand for betryggende fortolkning.

De metoder der dermed blev indført kaldte Cardano og Bombelli som nævnt "sofistiske". Metoderne tillod også løsning af sådanne 2.gradsligninger, som man før ikke kunne stille noget op med (men som altså heller ikke har en fortolkelig løsning), f.eks. ligningen $x^2 + 2o = 8x$. Selv om aktørerne forsøgte sig med fortolkninger af hvad der går for sig - de taler f.eks. om $\sqrt{-121}$ som 11 forsynet med et særligt, nyt fortegn - lykkedes det ikke for dem,og heller ikke for efterfølgerne i de næste par hundrede år at nå til rimelige resultater.

Af den grund blev de "sofistiske tal", eller "de umulige tal", ikke i begyndelsen alment accepteret af matematikerne. Når de blev det på lidt længere sigt,var det i første omgang fordi de tilbyder en uimodståeligt tiltrækkende, endegyldig behandling af n'te gradsligninger (idet ethvert n'te grads polynomium har netop

n rødder, hvis man tillader komplekse løsninger). (I anden omgang skyldtes accepten accepten at man med de komplekse tal får et meget magtfuldt hjælpemiddel ved behandlingen af en mangfoldighed af matematiske spørgsmål - og senere fysiske spørgsmål.) Dette forhold begyndte at blive klart i begyndelsen af 16oo-tallet (Roth 16o8, Girard 1629), og der i den forbindelse at Descartes (1637) kalder de rødder som ikke er reelle for indbildte, imaginære, et ord der siden er blevet stående, i en lidt anden betydning. Leibniz (1646-1716) kaldte dem amfibier mellem væren og ikke væren. Det er Euler (17o7-83) der som den første skrev det typiske komplekse tal på formen $a + b\sqrt{-1}$, hvor a of b er sædvanlige reelle tal. Han viste at mængden af sådanne tal er stabile over for de fire regningsarter, og nåede i øvrigt en betydelig virtuositet i jongleringen med dem. Selve betegnelsen komplekse tal udmøntedes af Gauss, der også indførte den moderne betegnelse $a + ib$, hvor $i = \sqrt{-1}$ er den såkaldte imaginære enhed.

Men det blev ved med at være en pæl i kødet på matematikerne, at de komplekse tal ikke kunne indrammes af en betryggende fortolkning. Mange forsøg blev gjort, men først for Caspar Wessel (dansk-norsk, 1745-1818, bror til Hermann) lykkedes det, i afhandlingen "Om Directionens analytiske Betegning" (1797). Men hans arbejde forblev upåagtet indtil 1897, hvor det oversattes til fransk. Hans betragtninger udsprang af landmålingssproblemstillinger, og havde ikke fra starten noget med komplekse tal at gøre, men førte ud i dem. Essensen i hans arbejde var at indføre regning med hvad vi i dag kalder plane vektorer. De udstyres med (moderne) vektoraddition og med en multiplikationsoperation, hvorved to vektorer multipliceres ved at deres længder multpliceres, mens deres vinkler med en på forhånd givet enhedsvektor, som Wessel kaldte 1, adderes. Den enhedsvektor som fremgår af 1 ved drejningen $+90^{\circ}$ kaldte han ε. Med den indførte multiplikation bliver $\varepsilon^2 = -1$, den modsatte til den første enhedsvektor. Derved kan ε opfattes som en realisation af den imaginære enhed. Skønt længe ukendt er Wessels geometriske betragtningsmåde blevet fast inventar i omgangen med komplekse tal.

Det skyldes nok at den ikke var helt enestående i den matematiske verden. Nogenlunde samtidig arbejdede franskmanden Carnot og scweizeren Argand med lignende forestillinger. Men frem for alt gjaldt dette Gauss som i sit bevis (fra 1797) - det første

korrekte - for algebraens fundamentalsætning (at enhver n'te gradsligning i de komplekse tal har en rod) opererede med en repræsentation af de komplekse tal i planen (hvorved den kaldes den komplekse plan), som for alvor blev gængs efter et arbejde af Gauss fra 1831.

Disse geometriske fortolkninger af de komplekse tal var imidlertid ikke de eneste mulige. I sin Cours d'Analyse fra 1821 anskuer Cauchy (1789-1857) de komplekse tal som rent formelle størrelser underkastet bestemte regneregler. Disse størrelser havde imidlertid ikke nogen reel fortolkning, han siger "en imaginær ligning er udelukkende den symbolske fremstilling af to ligninger mellem reelle størrelser". Cauchy's opfattelse indeholder i svøb det moderne algebraiske begreb om de komplekse tal som par af reelle tal, på hvilke der er defineret en additions- og en multiplikationsoperation. End fuld udarbejdelse af dette begreb blev givet af Hamilton (18o5-65) i 1833, i en konstruktion hvor de komplekse tal danner et kommutativt legeme (i vores sprogbrug). Det er i det store hele denne konstruktion vi skal gennemføre i det følgende. Hamilton gik et skridt videre og konstruerede et ikke-kommutativt legeme med tre imaginære (samt en reel) enhed, de såkaldte kvaternioner, som vi dog ikke skal komme nærmere ind på i denne fremstilling.

Med Hamilton var indførelsen af de komplekse tal helt henført til de reelle tal. Det forhold at afklaringen af de øvrige, simplere, talområders status kommer meget senere i århundredet antyder at der dér er mere grundlæggende filosofiske vanskeligheder på spil end ved de ved første øjekast langt mere utilnærmelige komplekse tal.

Man kan begrunde definitionen af multiplikationen på flere måder, men de har alle præg af efterrationalisering i et eller andet omfang, idet de på én eller anden måde foregriber det de komplekse tal skal kunne (og faktisk kan). Vi vil nøjes med at skitsere Hamilton's begrundelse:

Organiserer vi først R^2 med en skalarmultiplikation bestemt ved $r(a_1,a_2) = (ra_1,ra_2)$ når $r \in R$, har vi at

$$(a_1,a_2) = a_1(1,o)+a_2(o,1).$$

Forlanger vi dernæst at (1,o) skal være neutralt element ved multiplikationen, og at multiplikationen i øvrigt skal være distributiv over for +, må vi have

$$(a_1,a_2)\cdot(b_1,b_2) = a_1b_1(1,o)+(a_2b_1+a_1b_2)(o,1)+a_2b_2(o,1)^2.$$

Nu må, da jo $(o,1)^2$ skal resultere i et par, $(o,1)^2 = (a,b)$ for passende $a,b \in R$. Men hvilke? Hamilton forlangte, at længden af et produkt skal være lig produktet af faktorernes længder, hvor længde$(x,y) = \sqrt{a^2+b^2}$. Med dette krav følger, idet

$$(1,1)\cdot(1,-1)=((1,o)+(o,1))\cdot((1,o)-(o,1)) = (1,o)^2-(o,1)^2$$
$$= (1,o)-(o,1)^2 = (1,o)-(a,b) = (1-a,b),$$

dels at længde$((1,1)\cdot(1,-1))$ = længde$(1,1)\cdot$længde$(1,-1) = \sqrt{2}^2 = 2$, dels videre, at

$$2 = \text{længde}((1,1)\cdot(1,-1)) = \text{længde}\,(1-a,b) = \sqrt{(1-a)^2+b^2},$$

så at $(1-a)^2+b^2 = 4$. Samtidig må

$$\sqrt{a^2+b^2} = \text{længde}(a,b) = \text{længde}(o,1)^2 = (\text{længde}(o,1))^2 = 1,$$

altså $a^2+b^2 = 1$. Løsningerne til disse to ligninger i a og b er a = -1 og b = o, hvorved $(o,1)^2 = (-1,o) = -(1,o)$.

Konstruktionen af de komplekse tal

I den ramme vi her har valgt fremstilles de komplekse tal som mængden af reelle talpar forsynet med to bestemte kompositioner, + og ·. Disse indføres således:

Definition: For $(a_1,a_2), (b_1,b_2) \in R^2$ sætter vi

$$(a_1,a_2) + (b_1,b_2) = (a_1+b_1,a_2+b_2),$$
$$(a_1,a_2)\cdot(b_1,b_2) = (a_1b_1-a_2b_2,a_2b_1+a_1b_2).$$

Definitionsmæssigt set er et komplekst tal altså blot et reelt talpar, men for at understrege at den her indførte multiplikation er i spil skriver vi C i stedet for R^2. Vi vil nu godtgøre, at $(C,+,\cdot)$ er et kommutativt legeme.

Først observerer vi, at $(C,+)$ er en kommutativ gruppe, med $0 = (o,o)$ som neutralt element.

At C er stabil over for +, og at + er kommutativ og associativ er oplagt. Klart er det også, at (o,o) er neutralt ved +, og at $(-a_1,-a_2)$ er inverst ved + til (a_1,a_2). Disse egenskaber følger alle direkte af egenskaberne ved addition i R.

Endvidere er $(C\setminus\{o\},\cdot)$ en kommutativ gruppe med $1 = (1,o)$ som neutralt element.

Dette er også let at se, men lidt mindre banalt end det foregående. Dog er stabiliteten af C over for · samt kommutativiteten af · åbenbare.

Associativiteten: Vi har

$$((a_1,a_2)\cdot(b_1,b_2))\cdot(c_1,c_2) = (a_1b_1-a_2b_2,a_2b_1+a_1b_2)\cdot(c_1,c_2)$$
$$= (a_1b_1c_1-a_2b_2c_1-a_2b_1c_2-a_1b_2c_2,a_2b_1c_1+a_1b_2c_1+a_1b_1c_2-a_2b_2c_2)$$

og

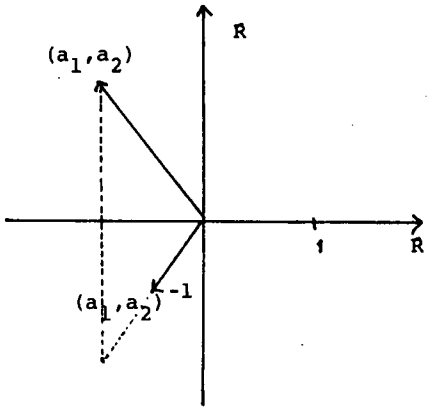
$$(a_1,a_2)\cdot((b_1,b_2)\cdot(c_1,c_2)) = (a_1,a_2)\cdot(b_1c_1-b_2c_2,b_2c_1+b_1c_2)$$
$$= (a_1b_1c_1-a_1b_2c_2-a_2b_2c_1-a_2b_1c_2,a_2b_1c_1-a_2b_2c_2+a_1b_2c_1+a_1b_1c_2).$$

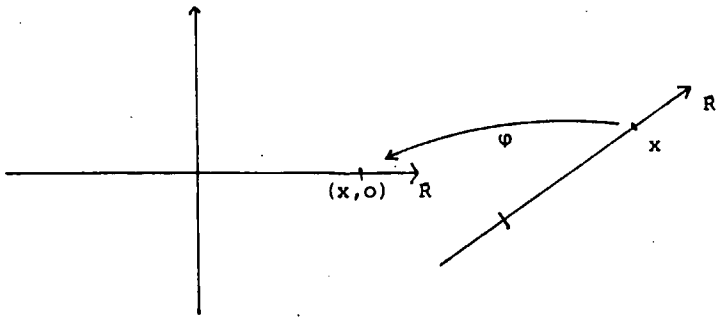
Identiteten af de to slutudtryk viser identiteten af de to begyndelsesudtryk.

(1,o) er neutralt, thi $(a_1,a_2)\cdot(1,o) = (a_1\cdot1-a_2\cdot o,a_2\cdot1+a_1\cdot o)$ $= (a_1,a_2)$ (multiplikationen i den omvendte orden er overflødig på grund af kommutativiteten).

Ethvert element $\neq (o,o)$ har et inverst. Lad nemlig (a_1,a_2) $(\neq (o,o))$ være givet. Skal (x_1,x_2) være inverst til (a_1,a_2)

Man kunne sagtens ved at sno sig en anelse mere løse ligningssystemet konkret her og nu uden at påberåbe sig generel ligningsteori.





må $(1,o) = (a_1,a_2)\cdot(x_1,x_2) = (a_1x_1-a_2x_2, a_2x_1+a_1x_2)$,
dvs.

$a_1x_1-a_2x_2 = 1$
$a_2x_1+a_1x_2 = o.$

Dette ligningssystem i x_1 og x_2 har netop én løsning, da dets koefficientmatrix har determinanten $a_1^2+a_2^2$, som er forskellig fra nul, da $(a_1,a_2) \neq (o,o)$. Hvis (x_1,x_2) løser dette system, da også systemet

$a_1a_2x_1-a_2^2x_2 = a_2$
$-a_1a_2x_2-a_1^2x_2 = o,$

der ved addition giver $-(a_1^2+a_2^2)x_2 = a_2$, altså

$x_2 = -a_2/(a_1^2+a_2^2)$.

På tilsvarende måde finder vi

$x_1 = a_1/(a_1^2+a_2^2)$.

At parret (x_1,x_2) defineret således faktisk løser det oprindelige system ses umiddelbart ved indsættelse.

Vi noterer os som et selvstændigt resultat, at <u>det inverse element ved · til (a_1,a_2)</u> har formen

(1) $(a_1,a_2)^{-1} = (a_1/(a_1^2+a_2^2), -a_2/(a_1^2+a_2^2))$, $(a_1,a_2) \neq (o,o)$.

For at have fuldført demonstrationen af, at $(C,+.\cdot)$ er et kommutativt legeme mangler vi blot at indse, at · er distributiv med hensyn til +. Dette ses ved en enkel udregning:

$((a_1,a_2)+(b_1,b_2))\cdot(c_1,c_2) = (a_1+b_1,a_2+b_2)\cdot(c_1,c_2) =$
$(a_1c_1+b_1c_1-a_2c_2-b_2c_2, a_2c_1+b_2c_1+a_1c_2+b_1c_2)$
og
$(a_1,a_2)\cdot(c_1,c_2) + (b_1,b_2)\cdot(c_1,c_2) =$
$(a_1c_1-a_2c_2, a_2c_1+a_1c_2) + (b_1c_1-b_2c_2, b_2c_1+b_1c_2)$
$= (a_1c_1+b_1c_1-a_2c_2-b_2c_2, a_2c_1+b_2c_1+a_1c_2+b_1c_2),$

hvoraf distributiviteten fremgår (kommutativiteten af · fritager os for at betragte multiplikationen med (c_1,c_2) fra venstre).

Det er nu muligt at finde et eksemplar af de reelle tals legeme $(R,+,\cdot)$ <u>indlejret isomorft som dellegeme af $(C,+,\cdot)$</u>. Vi betragter afbildningen $\varphi: R \sim C$, defineret ved

$\varphi(x) = (x,o)$, $x \in R$.

Det er nemt at se, at der også gælder ting som $(c(a_1,a_2))(d(b_1,b_2)) = cd(a_1,a_2)(b_1,b_2)$, $(a/c,b/c) = \frac{1}{c}(a,b)$, foruds̄at, at c ikke er o, osv.

Denne afbildning φ er en injektiv homomorfi,

eftersom $x \neq y \Rightarrow \varphi(x) = (x,o) \neq (y,o) = \varphi(y)$,
og $\varphi(x+y) = (x+y,o) = (x,o) + (y,o) = \varphi(x) + \varphi(y)$,
samt $\varphi(xy) = (xy,o) = (xy-o\cdot o, o\cdot y+x\cdot o) = (x,o)\cdot(y,o)$
$= \varphi(x)\varphi(y)$.

Derfor er φ en isomorfi mellem R og $\varphi(R)$ $(= \{(x,o) \mid x \in R\})$, hvorfor vi tillader os at betragte R som en delmængde af de komplekse tal, eller anderledes sagt C som en udvidelse af R. Øjensynlig er $R \subset C$. I medfør af denne identifikation identificerer vi også i notationen det komplekse tal (x,o) med det reelle tal x. I kraft af det får vi for $c \in R$:

$$c(a_1,a_2) = (c,o)\cdot(a_1,a_2) = (ca_1-oa_2, oa_1+ca_2) = (ca_1,ca_2).$$

Specielt er $(-1)(a_1,a_2) = (-a_1,-a_2) = -(a_1,a_2)$.

Vi ser nu lidt nærmere på elementet (o,1) i C. Det noteres

$i = (o,1)$, den imaginære enhed.

Om i gælder, at $i^2 = (o,1)\cdot(o,1) = (o\cdot o-1\cdot 1, 1\cdot o+o\cdot 1) = (-1,o) = -1$. Denne bemærkelsesværdige egenskab - lad os give den en linje -

(2) $i^2 = -1$

bevirker at i C har ligningen $x^2+1 = o$ en løsning. Den har endda to, nemlig i og -i ($(-i)^2 = i^2 = -1$). Senere i kapitlet skal vi vende tilbage til de komplekse tals evne til at levere løsninger til enhver n'te gradsligning.

Ved hjælp af den imaginære enhed og indlejringen af R i C kan vi fremstille de komplekse tal på en lidt anden måde end før. Det komplekse tal $z = (a_1,a_2)$ skrives $z = (a_1,a_2) = (a_1,o) + (o,a_2) = a_1+a_2i$, eller ved ombytning af a_2 og i:

$z = a_1+ia_2$, $a_1,a_2 \in R$.

Der gælder tydeligvis: $a_1+ia_2 = b_1+ib_2 \Leftrightarrow (a_1,a_2) = (b_1,b_2)$ altså hvis og kun hvis $a_1 = b_1$ og $a_2 = b_2$.

Med denne skrivemåde fremstilles altså z som sum af et reelt tal, a_1, og et reelt multiplum af den imaginære enhed. Vi kalder a_1 for z's realdel, den skrives ofte Re(z). Tallet a_2 kaldes z's imaginærdel, a_2 = Im(z). Et kompleks tal af form ib

Dette kunne også udtrykkes

$$\mathrm{Re}(z^{-1}) = \frac{\mathrm{Re}(z)}{(\mathrm{Re}(z))^2+(\mathrm{Im}(z))^2}\ ,\quad \mathrm{Im}(z^{-1}) = \frac{-\mathrm{Im}(z)}{(\mathrm{Re}(z))^2+(\mathrm{Im}(z))^2}$$

Med denne tegning har vi brudt den ramme vi arbejder i. Men det er ikke så farligt, da ingen af betragtningerne (de formelle dele af dem) i det følgende beror på denne tegning. Repræsentationen viser i øvrigt, at vi kan tænke på det komplekse tal z = a+ib som (sted)vektoren (a,b).

Det ville ikke have hjulpet os at betragte en total, refleksiv ordning, harmonerende med + og ·, da vi ud fra den kunne skaffe en irrefleksiv af den behandlede type.

kaldes rent imaginært.

I denne notation, som vi vil benytte fra nu af, har vi (check selv):

$$(a+ib)+(c+id) = (a+c)+i(b+d),\quad (a+ib)(c+id) = (ac-bd)+i(bc+ad).$$

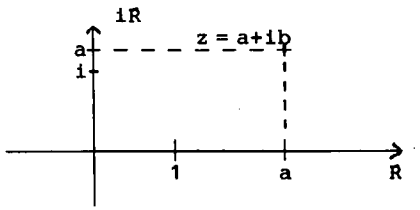
Vi tillader os også at skrive

$$\frac{1}{z} = \frac{1}{a+ib} \text{ for } z^{-1} \quad (z \neq o).$$

Af (1) får vi

$$\frac{1}{a+ib} = \frac{a-ib}{a^2+b^2}\ .$$

Det forhold at elementerne i C er par af reelle tal, bevirker at vi ikke tænker på C som en tallinje, men som en plan, den komplekse plan. Første-aksen er at opfatte som R. Den indeholder ételementet 1 = (1,o), mens anden-aksen, kaldes den imaginære akse. Den benævnes ofte i denne sammenhæng iR, fordi den indeholder den imaginære enhed i.



Der er endnu en grund til at tænke på de komplekse tal som udgørende en plan (en tredje gives i et senere afsnit), frem for som en tallinje. Det er nemlig umuligt at ordne C fornuftigt (dvs. for den irrefleksive udgave: trichotymisk og i harmoni med kompositionerne + og ·). Var nemlig en sådan ordningsrelation måtte der for ethvert $z \neq o$ gælde $z > o$ eller $z < o$. I begge tilfælde ville $z^2 > o$. Ser vi specielt på 1 og i fås at $1^2 > o$ og $i^2 > o$. Ved addition (og harmoni) måtte så $o = 1+i^2 = 1^2+i^2$ samtidig med at $1^2+i^2 > o$, hvilket ikke lader sig realisere med en irrefleksiv ordningsrelation. Selv om vi ikke kan ordne C, og selv om vi tidligere har benyttet ordning til at definere numerisk værdi, kan vi alligevel i C etablere et rimeligt begreb om numerisk værdi. Det sker i det næste afsnit.

Vi har dog endnu et ærinde at gøre i dette. Tillader vi os at inddrage lidt lineær algebra kan vi anskue C som et vektorrum over de reelle tals legeme. (C,+) er jo en kommutativ gruppe, og afbildningen

Gå selv disse egenskaber efter. ⟶

Vi kan også opfatte C som vektorrum over C selv som skalarlegeme. Da C er et legeme bliver selvfølgelig ethvert {z} , $z \neq o$, en basis for (C,+,·,C), som altså er 1-dimensionalt.

Gangen i beviset er at supplere 1 med et $c \in L \setminus R$, så at {1,c} er en basis for L. Derefter finder vi et element i L, som ikke er reelt, men hvis kvadrat er negativt reelt. Det viser sig, at vi kan finde et $\beta \in R$, så at c-β har netop denne egenskab. Tilbage står så blot at "normere" c-β så det resulterende element har -1 som kvadrat.

$(\lambda,z) \rightsquigarrow \lambda z, \lambda \in R, z \in C$

opfylder kravene til skalamultiplikation med (R,+,·) som skalarlegeme, eftersom (C,+,·) er et legeme, der indeholder R. Eftersom ethvert komplekst tal z har fremstilllingen z = a+ib = a·1+b·i som linearkombination af de to elementer 1 og i, udspæder disse C. De er samtidig lineært uafhængige, fordi a+ib = o hvis og kun hvis a = o og b = o. Derfor udgør {1,i} en basis for C over R. Det bevirker, at vektorrummet (C,+,·,R) har dimensionen 2. Med disse betragtninger til rådighed kan vi formulere et entydighedsresultat om C. Det indgår sammen med en opsummering af hvad vi i det foregående har opnået i

Sætning V.1. Med $C = R^2$ forsynet med de ovenfor indførte kompositioner + og · er (C,+,·) et kommutativt legeme, der indeholder (R,+,·) (på nær isomorfi) som dellegeme.

Med den ovenfor indførte skalarmultiplikation kan C endvidere opfattes som et vektorrum over de reelle tal af dimension 2.

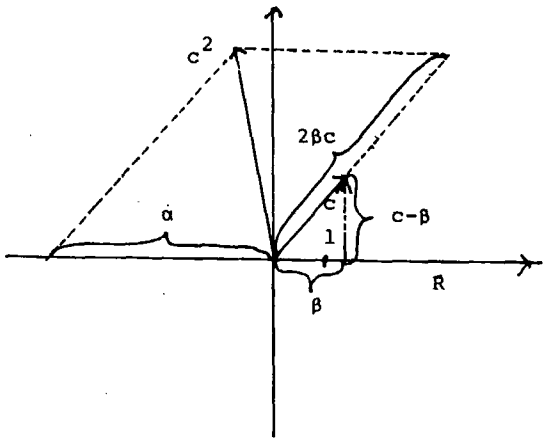
Hvis (L,+,·) er et kommutativt legeme med (R,+,·) som dellegeme (på nær isomorfi), der kan opfattes som et to-dimensionalt vektorrum over R, er legemet (L,+,·) isomorft med (C,+,·). I denne forstand er altså (C,+,·) entydigt bestemt.

Bevis.

De to første punkter er bevist i gennem de foregående betragtninger. Vi mangler blot det sidste punkt.

Idéen er at finde i L en pendant til den imaginære enhed i i C, for derefter at skabe isomorfien mellem C og L ved at lade z i C, z = a+ib, afbilde i linearkombinationen af 1 og i's pendant med a, henholdsvis b som koefficienter. I detaljer går vi således til værks:

Da L er to-dimensionalt og $1 \in R$ ikke er 0, kan suppleres med et element c fra L til en basis {1,c} for L. Dette element c må ligge i $L \setminus R$, thi var c i R ville 1 og c være lineært afhængige ($o = 1 + (-\frac{1}{c})c$). Vi betragter nu elementet $c^2 \in L$. Da {1,c} er en basis for L findes koefficienter α og $\beta \in R$, så at



Det ville være mere naturligt blot at skrive $c^2 = \alpha + \beta c$, men af hensyn til det følgende er det lidt mere bekvemt at kalde koefficienten til c for 2β.

ψ virker ved at et tal $z \in C$ med realdel a og imaginærdel b sendes over i linearkombinationen af 1 og j med koefficienterne a og b.

$$c^2 = \alpha + 2\beta c.$$

Da $\beta \in R$ er <u>c-β ikke element</u> i R (ellers ville jo $c = (c-\beta)+\beta$ tilhøre R). Til gengæld er c-β's kvadrat element i R, da

$$(c-\beta)^2 = c^2+\beta^2-2c\beta = \alpha+2\beta c+\beta^2-2c\beta = \alpha+\beta^2 \in R.$$

Der må så gælde, at $(c-\beta)^2 < o$. Var nemlig alternativt $(c-\beta)^2 \geq o$, ville der findes (Sætning IV.1o.) et $\rho \in R$, så at $\rho = \sqrt{(c-\beta)^2}$. Det vil sige, at c-β løste ligningen $x^2 = \rho^2$, og dermed ligningen $(x-\rho)(x+\rho) = o$, der (fordi $(L,+,\cdot)$ er et legeme) kun har løsningerne $x = \rho$ og $x = -\rho$, der begge er reelle.

Når $(c-\beta)^2 < o$ er $-1/(c-\beta)^2 > o$. Derfor findes et $\sigma \in R_+$, så at $\sigma^2 = -1/(c-\beta)^2$. Sætter vi nu $j = \sigma(c-\beta)$ er $j^2 = \sigma^2(c-\beta)^2 = -1$. Øjensynlig kan j ikke tilhøre R, da i så fald $c-\beta = \frac{j}{\sigma} \in R$, i strid med at $c-\beta \notin R$. Så må også 1 og j være lineært uafhængige. Thi hvis $a+jb = o$ for $(a,b) \neq (o,o)$ måtte $b \neq o$, for var $b = o$ ville også $a = o$. På den anden side kan det heller ikke lade sig gøre at $b \neq o$, for så ville $j = -\frac{a}{b} \in R$, i strid med at $j \notin R$. Dermed er $\{1,j\}$ en basis for L.

Således har vi i j fundet en pendant til i.

Afbildningen $\psi: C \rightsquigarrow L$, defineret ved

$$\psi(z) = \psi(a+ib) = a+jb,$$

når $z = a+ib$, $a,b \in R$, er en <u>isomorfi mellem $(C,+,\cdot)$ og $(L,+,\cdot)$</u>.

<u>Surjektiviteten</u> følger af: $\ell \in L \Rightarrow \ell = a+jb$, så at $\ell = \psi(a+ib)$.
<u>Injektiviteten</u>: $\psi(z_1) = \psi(z_2)$ $(z_1=a_1+ib_1,\ z_2 = a_2+ib_2)$ medrer, at $a_1+jb_1 = a_2+jb_2$, hvoraf $(a_1-a_2)+j(b_1-b_2) = o$, som på grund af den lineære uafhængighed af 1 og j afstedkommer, at $a_1 = a_2$ og $b_1 = b_2$, altså at $z_1 = z_2$.
Endelig <u>homomorfien</u>: $\psi(z_1+z_2) = \psi((a_1+a_2)+i(b_1+b_2))$
$= (a_1+a_2)+j(b_1+b_2) = (a_1+jb_1)+(a_2+jb_2) = \psi(z_1) + \psi(z_2)$,
og
$\psi(z_1z_2) = \psi((a_1+ib_1)(a_2+ib_2)) = \psi(a_1a_2-b_1b_2+i(b_1a_2+a_2b_1))$
$= (a_1a_2-b_1b_2)+j(b_1a_2+a_2b_1) = (a_1+jb_1)(a_2+jb_2) = \psi(z_1)\ \psi(z_2)$.
Q.E.D.

Hermed er sætningen bevist.

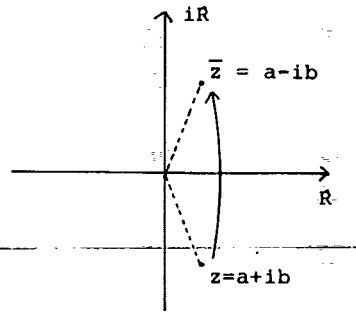
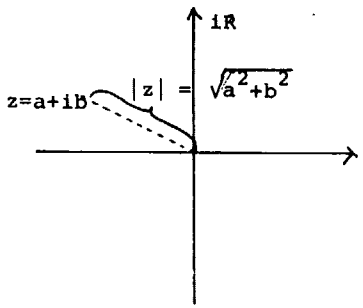


Illustration af konjugering.

Læg mærke til at der heraf følger at både $z+\bar{z}$ og $z\bar{z}$ er reelle for ethvert $z \in C$.



Egenskaberne (i)-(iv) i Sætning V.2. viser, at $|\ |_C$ er en norm i C (både som vektorrum over R og over C, idet (iv) viser at normen af et (reelt respektive komplekst) skalarmultiplum af et elemenet i C er den numeriske værdi af skalaren gange med normen af elementet).

Yderligere træk ved de komplekse tal

Sammen med det komplekse tal z = a+ib studeres ofte det nært beslægtede

$$\bar{z} = a-ib,$$

der kaldes det konjugerede til z. Svarende hertil kaldes afbildningen $k: C \rightsquigarrow C$, defineret ved $k(z) = \bar{z}$ for konjugering(s-afbildningen). Øjensynlig gælder $z = \bar{z}$ netop hvis a+ib = a-ib, altså netop hvis 2ib = o, dvs. præcis når z er reel. Afbildningen k er en isomorfi af C på sig selv.

Den er injektiv. Thi for z = a+ib, w = c+id vil a-ib = c-id afstedkomme, at a = c og b = d, altså at z = w.
Den er surjektiv, fordi a+ib er billede af a-ib. Endelig skyldes homomorfien, at
$\overline{z+w} = \overline{(a+c)+i(b+d)} = (a+c)-i(b+d) = (a-ib)+(c-id) = \bar{z}+\bar{w}$,
og
$\overline{zw} = \overline{(a+ib)(c+id)} = ac-bd+i(bc+ad) = (ac-bd)-i(bc+ad)$,
samtidig med, at
$\bar{z}\bar{w} = (a-ib)(c-id) = ac-bd-i(bc+ad)$.

Vi lægger mærke til, at $\bar{\bar{z}} = z$, altså at kok = i (vi siger, at k er idempotent).

Det er nu tiden at indføre en numerisk værdi.

Definition: For $z \in C$ forstås ved den numeriske værdi af z det reelle tal

$$|z|_C = \sqrt{a^2+b^2} \qquad (z = a+ib).$$

Definitionen giver mening, fordi $a^2+b^2 \geq o$, således at kvadratroden eksisterer, jfr. Sætning IV.1o.

Da $z\bar{z} = (a+ib)(a-ib) = a^2-(ib)^2 = a^2+b^2$, er $|z|_C = \sqrt{z\bar{z}}$.

Berettigelsen af at bruge betegnelsen numerisk værdi ses af

Sætning V.2. Den numeriske værdi er en afbildning $|\ |_C: C \rightsquigarrow R$ med følgende egenskaber:
(i) $|z|_C \geq o$ for alle $z \in C$
(ii) $|z|_C = o \Leftrightarrow z = o$

(iii) $|z+w|_C \leq |z|_C + |w|_C$ for alle $z,w \in C$ (trekantsuligheden)

(iv) $|zw|_C = |z|_C|w|_C$ for alle $z,w \in C$

Endvidere er $|\ |_C$ en udvidelse af $|\ |$ på $\mathbb{R}$ som indført tidligere, dvs. hvis $x \in \mathbb{R}$ er $|x|_C = |x|$.

Bemærkning: På grund af det sidste punkt er der - når det er besvist ingen grund til at skelne notationsmæssigt mellem $|\ |_C$ og $|\ |$.

Bevis:

For at slippe typografisk billigst viser vi det sidste punkt først: For $x \in \mathbb{R}$ er $|x|_C^2 = x^2$. Samtidig er $|x|^2 = x^2$. Det viser, at $|x|_C$ og $|x|$ begge er ikke-negative løsninger til ligningen $y^2 = x^2$. Den har (med x^2 på α's plads) i følge Sætning IV.1o netop én ikke-negativ løsning. Men så må $|x|_C = |x|$.

Derefter tager vi fat på de øvrige punkter, hvor punkt (i) er trivielt ud fra definitionen. Klart er det også, at ($z = a+ib$) $|z| = 0 \Leftrightarrow a^2+b^2 = 0 \Leftrightarrow a = 0$ og $b = 0 \Leftrightarrow z = 0$. Det var punkt (ii).

Også punkt (iv) følger let: for $z = a+ib$, $w = c+id$ er

$$(|z||w|)^2 = (a^2+b^2)(c^2+d^2) = a^2c^2+b^2c^2+a^2d^2+b^2d^2$$

og

$$|zw|^2 = (ac-bd)+i(bc+ad)^2 = (ac-bd)^2+(bc+ad)^2$$
$$= a^2c^2+b^2d^2-2acbd+b^2c^2+a^2d^2+2bcad = a^2c^2+b^2d^2+b^2c^2+a^2d^2,$$

hvoraf identiteten mellem $(|z||w|)^2$ og $|zw|^2$ fremgår. At derefter $|z||w| = |zw|$ skyldes endnu engang Sætning IV.1o.

Det er lidt mere omstændeligt - men ikke af den grund svært - at vise trekantsuligheden (iii). Den er ækvivalent med, at

$$|z+w|^2 \leq |z|^2+|w|^2+2|z||w|.$$

Men med $z = a+ib$ og $w = c+id$ er

$$|z+w|^2 = |((a+c)+i(b+d)|^2 = (a+c)^2+(b+d)^2 =$$
$$a^2+c^2+2ac+b^2+d^2+2bd = |z|^2+|w|^2+2(ac+bd) \leq |z|^2+|w|^2+2|z||w|,$$

hvor lighedstegnene alle er oplagte, og hvor det springende punkt ligger i den afsluttende ulighed, der jo kommer ud på at

Strengt taget fordrer selve opskrivning af kvadratroden (endnu) at w^2 er reel, hvilket sikres af at w er det.

$(ac+bd) \leq |z||w|$. Dette indser vi på denne måde:

$$|z||w| = \sqrt{(ac-bd)^2+(bc+ad)^2} = \sqrt{(ac+bd)^2+(bc-ad)^2}$$

(de dobbelte produkter hørende til de to parenteser er ens i de to kvadratrødder)

$$\geq \sqrt{(ac+bd)^2} = |ac+bd| \geq ac+bd.$$

Hermed er sætningen bevist.

En direkte følge af denne sætning er det, at

$$\left|\frac{z}{w}\right| = \frac{|z|}{|w|} \quad \text{for } z,\ w \in C,\ w \neq 0.$$

Dette indses i to skridt. Hvis først $w \in R$, og $z = a+ib$, er

$$\frac{z}{w} = \frac{a}{w} + i\frac{b}{w} \quad (\tfrac{a}{w}, \tfrac{b}{w} \in R), \text{ hvorved}$$

$$\left|\frac{z}{w}\right| = \sqrt{a^2/w^2+b^2/w^2} = \sqrt{(a^2+b^2)/w^2} = \frac{1}{|w|}\sqrt{a^2+b^2} = \frac{|z|}{|w|},$$

hvor det næstsidste lighedstegn følger af at w er reel.
Er dernæst $w \in C$, $w = c+id$, er

$$\frac{z}{w} = \frac{z}{c+id} = \frac{z(c-id)}{(c+id)(c-id)} = \frac{z(c-id)}{c^2+d^2} = \frac{z(c-id)}{|w|^2},$$

hvorved i følge det første skridt

$$\left|\frac{z}{w}\right| = \left|\frac{z(c-id)}{|w|^2}\right| = \frac{|z||(c-id)|}{|w|^2} = \frac{|z||w|}{|w|^2} = \frac{|z|}{|w|},$$

hvor vi ved det næstsidste lighedstegn benyttede, at et kompleks tal og dets konjugere åbenbart har samme numeriske værdi.

Ved hjælp af den numeriske værdi kan man tale om og behandle grænseforhold for følger af komplekse tal. Herunder kan man definere konvergente følger og fundamentalfølger som kopier af de tilsvarende definitioner for reelle talfølger (se side), ligesom de herom gældende sætninger og deres beviser kan kopieres for komplekse følger.

Der gælder nu, at følgen $(z_n)_n = (a_n+ib_n)_n$ fra C er konvergent med grænseværdi a+ib, hvis og kun hvis realdelsfølgen $(a_n)_n$ er konvergent i R med grænseværdien a, og imaginærdelsfølgen $(b_n)_n$ er konvergent i R med grænseværdien b. Vi har nemlig, at

$$|z_n-z| = \sqrt{(a_n-a)^2+(b_n-b)^2},$$

hvorved

Lidt flere detaljer: Den første ulighed skyldes, at

$$|a_n-a|^2 \leq |a_n-a|^2+|b_n-b|^2,$$

hvorved

$$|a_n-a| \leq \sqrt{|a_n-a|^2+|b_n-b|^2}.$$

Tilsvarende med $|b_n-b|$. Den sidste ulighed følger af, at

$$|a_n-a|^2+|b_n-b|^2 \leq |a_n-a|^2+|b_n-b|^2+2|a_n-a||b_n-b| = (|a_n-a| + |b_n-b|)^2.$$

$$(3)\quad \left.\begin{matrix}|a_n-a|\\ |b_n-b|\end{matrix}\right\} \leq \sqrt{|a_n-a|^2+|b_n-b|^2} = |z_n-z| = \sqrt{|a_n-a|^2+|b_n-b|^2} \leq |a_n-a|+|b_n-b|.$$

Hvis derfor $z_n \to z$ for $n \to \infty$, vil også $a_n \to a$ og $b_n \to b$ for $n \to \infty$. For til et givet $\varepsilon > 0$ findes jo så et n_o så at $|z_n-z| < \varepsilon$ for $n \geq n_o$. I kraft af (3) vil så også $|a_n-a| < \varepsilon$ og $|b_n-b| < \varepsilon$ for $n \geq n_o$.

Er omvendt $(a_n)_n$ og $(b_n)_n$ konvergente med grænsepunkter henholdsvis a og b, og er $\varepsilon > 0$ givet, findes et n_o, så at for $n \geq n_o$: $|a_n-a| < \frac{1}{2}\varepsilon$ og $|b_n-b| < \frac{1}{2}\varepsilon$. Men så vil for de samme n

$$|z_n-z| \leq |a_n-a|+|b_n-b| < \tfrac{1}{2}\varepsilon+\tfrac{1}{2}\varepsilon = \varepsilon, \text{ (på grund af (3))},$$

hvorfor $z_n \to z$ for $n \to \infty$.

På helt tilsvarende måde godtgøres ud fra de med (3) parallelle uligheder

$$\left.\begin{matrix}|a_n-a_m|\\ |b_n-b_m|\end{matrix}\right\} \leq |z_m-z_n| \leq |a_n-a_m|+|b_n-b_m|,$$

at $(z_n)_n$ er en fundamentalfølge hvis og kun hvis dens realdels- og imaginærdelsfølger $(a_n)_n$ og $(b_n)_n$ begge er fundamentalfølger i $\mathbb{R}$.

Dette resultat gør det muligt at besvare det nærliggende spørgsmål om C udgør et fuldstændigt (men altså ikke ordnet!) legeme, altså om enhver fundamentalfølge er konvergent i C. Svaret er bekræftende. Thi hvis $(z_n)_n = (a_n+ib_n)_n$ er en fundamentalfølge gælder følge det ovenstående det samme om $(a_n)_n$ og $(b_n)_n$ i $\mathbb{R}$. Men da disse følger er reelle er de konvergente i $\mathbb{R}$, med grænseværdier henholdsvis a og b. Men så er - endnu engang i kraft af det ovenstående - også $(z_n)_n$ konvergent med grænseværdien a+ib. Dette resultat fortjener vist ophøjelse til sætning:

Sætning V.3. Med den ovenfor indførte numeriske værdi bliver enhver fundamentalfølge i C konvergent i C. Legemet C er altså fuldstændigt.

I den klassiske udvikling af teorien for disse funktioner, kom rækkeudviklingerne

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \dots \ , \quad \sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots$$

og

$$e^x = 1 + \frac{x^1}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

på et relativt sent stadium i udforskningen af deres egenskaber. Men de kan altså bruges som udgangspunkt for en definition af dem.

Grundene til at vi kan tillade os denne suggestive navngivning fremgår om lidt.

I de følgende afsnit vil vi indvinde nogle få af de egenskaber ved de komplekse tal, som berettiger dem til deres centrale stilling i matematikken. Til den ende er det nødvendigt at gå lidt uden for den opbygningsramme som er sat for denne fremstilling. Nærmere bestemt er vi nødt til at inddrage begreber og resultater som ikke er funderet i den opbygning vi allerede har foretaget. Det drejer sig om sinus- og cosinusfunktionerne (og i den forbindelse tallet π) og om eksponentialfunktionen, og om de vigtigste egenskaber ved disse funktioner, samt om begreber og resultater vedrørende kontinuerte funktioner. Faktisk ville det være muligt at udbygge det her opstillede grundlag, så disse ting kunne indfanges af det. Det ville imidlertid kræve nogle armbøjninger som det ville føre for vidt at tage i denne sammenhæng. I stedet nøjes vi med at præcisere de forudsætninger vi gør, og som går ud over rammen.

Polære koordinater. Produktets geometri

Vi lægger ud med at forudsætte de reelle funktioner cos og sin samt eksponentialfunktionen exp for givet, og deres egenskaber for kendt. (Skulle vi have defineret dem her, kunne det være sket med udgangspunkt i deres rækkeudviklinger:

$$\cos x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!} \ , \quad \sin x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}, \quad x \in \mathbb{R}$$

$$e^x = \exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \ x \in \mathbb{R}$$

hvor det så skulle godtgøres, at de pågældende rækker faktisk er konvergente for alle $x \in \mathbb{R}$, hvilket uden større vanskeligheder - men med lidt arbejde - lader sig gøre. Dernæst skulle vi ud fra disse definitioner have vist de egenskaber ved funktionerne vi får brug for; f.eks. skulle vi i den forbindelse have vist eksistensen af tallet π.)

Med disse forudsætninger definerer vi nu for $y \in \mathbb{R}$:

(4) $e^{iy} = \exp(iy) = \cos y + i \sin y$.

Af denne definition fremgår, at for $x \in \mathbb{R}$ er

$$\exp(ix) + \exp(-ix) = 2 \cos x, \quad \exp(ix) - \exp(-ix) = 2i \sin x,$$

hvoraf fremgår de såkaldte Euler's formler:

Ved hjælp heraf kan vi også definere cos og sin af komplekse variable, ved simpelthen i højresiden af (5) at lade x være kompleks, hvilket giver mening qua (6) (for z = a+ib er så exp(iz) = exp(-b+ia) = e^{-b}(cos a + i sin a)). Man kan i øvrigt vise, at på denne måde kommer de oven for nævnte rækkeudviklinger til at stemme også for komplekse værdier af x.

For dem der kender de hyperbolske funktioner giver det forhåbentlig en vis erkendelse at få nævnt, at

$\cos(ix) = \frac{1}{2}(e^{-x}+e^{-x}) = \cosh x$, og

$\sin(ix) = \frac{1}{2i}(e^{-x}-e^{x}) = -\frac{1}{i}(\frac{1}{2}(e^{x}-e^{-x}) = -\frac{1}{i}\sinh x.$

$$\text{(5)}\qquad \begin{aligned}\cos x &= \frac{e^{ix}+e^{-ix}}{2}\\ \sin x &= \frac{e^{ix}-e^{-ix}}{2i}\end{aligned}\qquad x \in \mathbb{R}$$

Det kan nævnes, at højre siderne er veldefinerede også for komplekse x. Det gør det muligt uden videre at definere cos og sin af komplekse værdier ved hjælp af formlerne (5).

Ud fra (4) kan vi definere også eksponentialfunktionen for komplekse værdier:

(6) $\exp(z) = \exp(x)\exp(iy) = e^{x}(\cos y + i \sin y)$, $z = x+iy$.

Den ses at stemme overens med den sædvanlig reelle eksponentialfunktion når z er reel, idet exp(io) = cos o = 1. Berettigelsen af benævnelsen eksponentialfunktion ligger - ud over i det netop nævnte forhold - i at der gælder

(7) $\exp(z+w) = \exp(z)\exp(w)$, $z,w \in \mathbb{C}$.

Dette vises under udnyttelse af additionsformlerne for cos og sin samt den for den reelle eksponentialfunktion gældende relation $e^{x+y} = e^{x}e^{y}$.

Vi har med z = x+iy og w = u+iv, at

$\exp(z+w) = \exp((x+u)+i(y+v)) = e^{x+u}(\cos(y+v)+i\sin(y+v))$

$= e^{x+u}((\cos u \cos v - \sin y \sin v) + i(\sin y \cos v + \cos y \sin v))$

og

$\exp(z)\exp(w) = e^{x}\exp(iy)e^{u}\exp(iv) =$

$e^{x+u}(\cos y + i \sin y)(\cos v + i \sin v) =$

$e^{x+u}(\cos y \cos v - \sin y \sin v + i(\sin y \cos v + \cos y \sin v)$,

hvoraf (7) fremgår.

Lad os i øvrigt bemærke, at der gælder $|\exp(z)| = |e^{x}| \geq o$,

idet $|\exp(z)| = |e^{x}||\cos y + i \sin y| = e^{x}(\cos^2 y+\sin^2 y) = e^{x}$.

Idet heltalspotenser af komplekse tal uden vanskeligheder defineres rekursivt som for reelle tal ($z^{o}=1$, $z^{n+1} = z^{n}z$, og for $z \neq o$: $z^{-n} = 1/z^{n}$, $n \in \mathbb{N} \cup \{o\}$) får vi af (7) ved induktion, at

(8) $\exp(pz) = (\exp(z))^{p}$, $p \in \mathbb{Z}$

For naturlige tal p indses påstanden ved induktion. Den er

Af (8) får vi nemt generelt, at $((\exp(z))^p)^q = (\exp(pz))^q = \exp(q(pz)) = \exp((pq)z) = (\exp(z))^{pq}$, for $p,q \in \mathbb{Z}$.

Abraham de Moivre (1667-1754), fransk-engelsk.

Dette afsnit tjener til at godtgøre at et vilkårligt punkt $(x,y) \in \mathbb{R}^2$ på enhedscirklen, har formen $(x,y) = (\cos\varphi, \sin\varphi)$ for et $\varphi \in \mathbb{R}$ (og alle andre vinkler der fremgår heraf ved addition af et heltalsmultiplum af 2π, men ingen andre). Dette er jo elementært (gymnasialt) stof, men da vi ikke vil forudsætte mere om cos og sin end det højst nødvendige, gives argumentet her.

tydeligvis sand for $n = 1$. Er den sand for $n = k$, så også for $n = k+1$, idet $\exp((k+1)z) = \exp(kz+z) = \exp(kz)\exp(z) = (\exp(z))^n\exp(z) = (\exp(z))^{k+1}$. For $p = o$ er den sand, fordi $\exp(o) = \cos o = 1$. For $-p \in \mathbb{N}$ er $\exp(pz)\exp((-p)z) = \exp(pz+(-p)z) = \exp(o) = 1$, hvorved $\exp(pz) = (\exp((-p)z))^{-1} = ((\exp(z))^{-p})^{-1} = (\exp(z))^p$.

Ved hjælp af dette fås umiddelbart de Moivre's formel:

(9) $\underline{(\cos x + i \sin x)^n = \cos nx + i \sin nx}$, $x \in \mathbb{R}$,

idet $(\cos x + i \sin x)^n = (\exp(ix))^n = \exp(nix) = \exp(inx) = \cos nx + i \sin nx$.

Vi er nu rustede til at angive en ny måde at fremstille de komplekse tal på.

Lad først x og y være reelle tal opfyldende, at $x^2+y^2 = 1$. Så er $o \leq x^2 = 1-y^2 \leq 1$, og dermed $-1 \leq x \leq 1$. For var $x > 1$ ville $x^2 > 1$, og var $x < -1$, ville $1 < -x$, altså $1 < (-x)^2 = x^2$. Da således $x \in [-1,1]$, og da cos: $\mathbb{R} \sim [-1,1]$ er surjektiv og periodisk med perioden 2π, findes et $\varphi \in \mathbb{R}$, så at $x = \cos\varphi$, og der gælder, for $u \in \mathbb{R}$, at $x = \cos u$ hvis og kun hvis $u = \varphi+p2\pi$, for et $p \in \mathbb{Z}$. Videre finder vi, at $\sin^2\varphi = 1 - \cos^2\varphi = 1-x^2 = y^2$, hvorved $\sin\varphi = y$ eller $\sin\varphi = -y$. I det første tilfælde har vi bestemt et $\varphi \in \mathbb{R}$, så at både $x = \cos\varphi$ og $y = \sin\varphi$. I det andet tilfælde sætter vi $\varphi' = -\varphi$. Så vil $\sin\varphi' = \sin(-\varphi) = -\sin\varphi = y$, og $\cos\varphi' = \cos(-\varphi) = \cos\varphi = x$, hvorved $x = \cos\varphi'$ og $y = \sin\varphi'$. Under alle omstændigheder har vi bestemt et $\varphi \in \mathbb{R}$, så at

$x = \cos\varphi$, $y = \sin\varphi$.

Da $\sin(\varphi+p2\pi) = \sin\varphi = x$, er for givne x og y φ entydigt bestemt på nær et additivt multiplum af 2π.

Med dette in mente betragter vi nu et vilkårligt komplekst tal z, $z = x+iy$, som opfylder, at $|z| = 1$, dvs. at $x^2+y^2 = 1$. I følge det foregående findes så $\varphi \in \mathbb{R}$ (entydigt bestemt på nær et additivt multiplum af 2π), så at $x = \cos\varphi$ og $y = \sin\varphi$. Det betyder at et $z \in \mathbb{C}$ med $|z| = 1$ har formen

Identiteten (1o) kan selvfølgelig også siges at stemme for $z = o$, idet højresiden er o uanset hvad φ er. At tillade $z = o$ på dette sted har imidlertid ikke megen mening, da der ikke på fornuftig måde til $z = o$ hører en vinkel φ. Der er derfor kotyme ikke at tillade $z = o$ i (1o).

Da jo f.eks. $\exp(iy) = \exp(i(y+p2\pi))$ for ethvert $p \in \mathbb{Z}$, $y \in \mathbb{R}$.

Denne fortolkning er netop den Caspar Wessel gav i 1797 (hans skrift herom udkom i 1799), som omtalt i indledningen til kapitlet.

$$z = \cos\varphi + i\sin\varphi,\ \varphi \in \mathbb{R}.$$

Er nu $z \in \mathbb{C}$ et vilkårligt kompleks tal, $\neq o$, vil om

$$z' = \frac{z}{|z|}$$

gælde, at $|z'| = |\frac{z}{|z|}| = \frac{|z|}{|z|} = 1$. Det viser, at z' falder ind under den foregående behandling. Det har altså formen

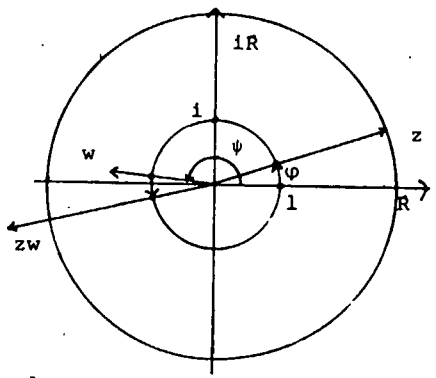
$$z' = \cos\varphi + i\sin\varphi,$$

for et $\varphi \in \mathbb{R}$. Så er $z = |z|z' = |z|(\cos\varphi + i\sin\varphi)$. Vi har altså for $z \in \mathbb{C}$, $z \neq o$, fremstillingen (1o) for et på nær et additivt multiplum af 2π entydigt bestemt $\varphi \in \mathbb{R}$:

(1o) $\underline{z = |z|(\cos\varphi + i\sin\varphi) = |z|e^{i\varphi}}$.

Man siger at z er fremstillet i <u>polære koordinater</u>. Da φ ofte kaldes tallet z's <u>argument</u> og $|z|$ dets <u>modulus</u>, siger man også at (1o) fremstiller z på modulus-argument form. Udnyttes at den reelle eksponentialfunktion $\exp: \mathbb{R} \to \mathbb{R}_+$ er bijektiv, får vi for $z \neq o$ (dvs. $|z| > o$), at der findes netop ét $\alpha \in \mathbb{R}$, så at $|z| = e^{\alpha}$. Ethvert komplekst tal forskelligt fra o kan altså skrives på formen $z = e^{\alpha}(\cos\varphi + i\sin\varphi) = \exp(\alpha+i\varphi)$, hvilket viser, at $\exp: \mathbb{C} \to \mathbb{C} \setminus \{o\}$ er surjektiv. (Derimod er den selvfølgelig ikke injektiv).

Fremstillingen af komplekse tal i polære koordinater lægger op til en <u>geometrisk fortolkning af det komplekse produkt</u>. Som tidligere repræsenteres $z = x+iy$ af punktet i planen med koordinaterne (x,y), og vi kan tænke på z som en vektor ud fra (o,o) med endepunkt (x,y). Tallet $\cos\varphi + i\sin\varphi$ repræsenteres så af en vektor med endepunktet $(\cos\varphi, \sin\varphi)$ på enhedscirklen. Denne vektor er karakteriseret ved at danne vinklen φ med 1. aksen (med sædvanlig omløbsretning i planen) og ved at have længden 1. Det almene komplekse tal z ($\neq o$) har så fremstillingen $z = |z|(\cos\varphi + i\sin\varphi)$, der repræsenteres af en vektor ud fra (o,o) af længden $|z|$ og dannende vinklen φ med 1.aksen. Multiplikationen af to komplekse



At der forholder sig sådan er ikke overraskende, når man betænker at multiplikationen i C af Hamilton netop er kalibreret til at have denne egenskab, jfr. kommentarerne til definitionen af · i begyndelsen af det andet afsnit i kapitlet.

Var $|z| > 1$ ville $|z|^n > 1$.(Et mere pedantisk gemyt kan overbevise sig herom med et trivielt induktionsbevis). Var alternativt $0 < |z| < 1$, ville tilsvarende $|z|^n < 1$.

se tal $z = |z|(\cos\varphi + i \sin\varphi)$ $(= |z|e^{i\varphi})$ og $w = |w|(\cos\psi + i \sin\psi)$ $(= |w|e^{i\psi})$, giver i kraft af de tidligere betragtninger resultatet

$$zw = |z|e^{i\varphi}\,|w|e^{i\psi} = |z||w|e^{i(\varphi+\psi)} = |z||w|(\cos(\varphi+\psi)+i\sin(\varphi+\psi)),$$

altså det komplekse tal, der som argument har summen af argumenterne for de to tal, og hvis modulus er produktet af de to indgående moduli.

Komplekse polynomier og deres rødder

Ved hjælp af fremstillingen af komplekse tal i polære koordinater kan vi give en simpel behandlingen af ligningen

$$z^n = 1,\ n \in \mathbb{N}.$$

Det er klart, at $z = 0$ ikke er rod i denne ligning. Vi kan derfor sætte $z = |z|(\cos\varphi + i \sin\varphi)$ for passende $\varphi \in R$. Ligningen kommer da ud på, at

$$1 = z^n = |z|^n(\cos\varphi + i \sin\varphi)^n = |z|^n(\cos n\varphi + i \sin n\varphi),$$

hvor vi til det sidste lighedstegn udnyttede de Moivre's formel. Da $|z|$ er et reelt tal opfyldende, at $|z| > 0$ og $|z|^n = 1$, er $|z| = 1$. Dvs. at ligningen er ækvivalent med de to ligninger $|z| = 1$ og $\cos n\varphi + i \sin n\varphi = 1$. Men her er den sidste ligning ensbetydende med, at $\cos n\varphi = 1$, dvs. at $n\varphi = p2\pi$, for et $p \in \mathbb{Z}$, altså m.a.o. $\varphi = p\frac{2\pi}{n}$, $p \in \mathbb{Z}$. Løsningen til ligningen er altså tallene z_p $(p \in \mathbb{Z})$ af formen

$$z_p = \cos p\tfrac{2\pi}{n} + i \sin p\tfrac{2\pi}{n}.$$

Vi vil nu nærmere undersøge, hvor mange forskellige af sådanne tal for $p \in \mathbb{Z}$ der findes. To af disse, z_p og z_q, er ens hvis og kun hvis $z_p z_q^{-1} = 1$ $(z_q \neq 0)$. Dette er ækvivalent med at

$$1 = e^{ip\frac{2\pi}{n}}\, e^{-iq\frac{2\pi}{n}} = e^{i(p-q)\frac{2\pi}{n}} = \cos(p-q)\tfrac{2\pi}{n} + i \sin(p-q)\tfrac{2\pi}{n},$$

der på sin side er ensbetydende med, at $(p-q)\frac{2\pi}{n}$ er et helt multiplum, $m2\pi$, af 2π:

$(p-q)\frac{2\pi}{n} = m2\pi$, for et $m \in \mathbb{Z}$, dvs. $p-q = mn$ for et $m \in \mathbb{Z}$.

Altså gælder, at

$z_p = z_q$ hvis og kun hvis $p-q$ er et helt multiplum af n.

Heraf ses, at for $p,q \in \{o,1,\ldots n-1\}$ er for $p \neq q$: $z_p \neq z_q$. Der gælder nemlig, at $o < p-q \leq n-1$, hvilket forhindrer, at $p-q$ kan være et helt multiplum af n. Tallene $z_o, z_1, \ldots z_{n-1}$ er altså indbyrdes forskellige. Er på den anden side p et helt tal, men $p \notin \{o,1,..,n-1\}$ vil vi vise, at z_p må være ét af tallene $z_o, z_1, \ldots z_{n-1}$. Vi sætter til den ende $m = [\frac{p}{n}]$. Så vil (se kapitel IV):

$$m = [\tfrac{p}{n}] \leq \tfrac{p}{n} < [\tfrac{p}{n}] + 1 = m+1,$$

hvorved $mn \leq p < mn+n$. Disse uligheder er ensbetydende med uligheder $o \leq p-mn < n$. Sættes så $q = p-mn$, vil $q \in \{o,1,\ldots n-1\}$. Da $p-q = mn$ (et helt multiplum af n) er $z_p = z_q$. Altså vil for $p \in \mathbb{Z} \setminus \{o,1,\ldots n-1\}$ z_p være lig netop ét af tallene $z_o, z_1, \ldots z_{n-1}$.

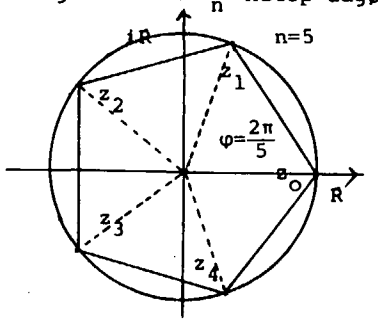
I alt har vi dermed vist

Sætning V.4. Ligningen $z^n = 1$ ($n \in \mathbb{N}$) har i $z \in \mathbb{C}$ netop n forskellige rødder, nemlig

$$z_p = e^{ip\frac{2\pi}{n}} \quad (= \cos p\tfrac{2\pi}{n} + i \sin p\tfrac{2\pi}{n}), \quad p = o,1,\ldots n-1$$

De kaldes de n n'te enhedsrødder.

De n n'te enhedsrødder har en nydelig geometrisk fortolkning, idet jo vinklen $\frac{2\pi}{n}$ netop udgør en n'te del af enhedscirkelbuen.



Det betyder, at n'te enhedsrødderne ligger på enhedscirklen som hjørnerne i en regulær n-kant, hvor første hjørne er 1.

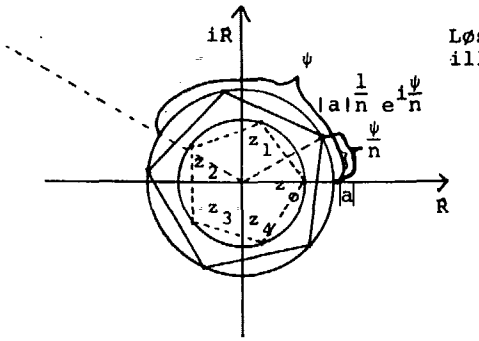
Vi kan herefter uden videre løse enhver ligning af formen

$$z^n = a, \text{ hvor } a \in \mathbb{C},\ n \in \mathbb{N}.$$

Ligningen er triviel hvis $a = o$. For $a \neq o$, og med $a = |a|e^{i\psi}$, er ligningen ækvivalent med ligningen

$$\frac{z^n}{|a|} e^{-i\psi} = 1,$$

Læg mærke til at vi her forudsætter, at vi kan uddrage (i R) den n'te rod af det positive reelle tal $|a|$. Det har vi faktisk aldrig vist, at vi kan. Det lader sig imidlertid gøre at modificere beviset for Sætning IV.1o. - der siger at ligningen $x^2 = a$ (for $a > o$) har netop én positiv løsning - til et bevis for, at enhver ligning $x^n = a$ ($a > o$, $n \in \mathbb{N}$) har netop én positiv løsning i R.



Løsningen af ligningen $z^n = a$ kan illustreres som på figuren (n = 5).

Hvis en kontinuert funktion f i en omegn A af et punkt a er o, så er den også o i a. Thi ellers var $|f(a)| > o$, og satte vi $\varepsilon = \frac{1}{2}|f(a)|$, fandtes på grund af kontinuiteten et $\delta > o$, så at $|(f(x)-f(a)| < \varepsilon$ for $x \in A$ og $|x-a| < \delta$. Men her er $|f(x)-f(a)| = |f(a)| > \varepsilon$ for $x \in A$, $x \neq o$. Da dette er i modstrid med det foregående, er $f(a) = o$. Vi har her benyttet dels definitionen på kontinuitet (overført til funktioner af en kompleks variabel), dels underforstået at et polynomium er kontinuert. Herved har vi faktisk begået et rammebrud, som vi kunne have repareret på ved at betale med endnu et par siders teori. Men det vil vi ikke.

For n = o: $p(z) = a_o$ er o for alle z netop hvis $a_o = o$. For n = 1: $p(z) = a_1 z + a_o = o$ for alle z, medfører, (med z = o), at $a_o = o$. Skal derefter $a_1 z = o$ for alle z, må $a_1 = o$.

og dermed med

$$(\frac{z}{|a|^{1/n}})^n e^{n(-i\frac{\psi}{n})} = 1.$$

Dette kommer ud på, at tallet $\frac{z}{|a|^{1/n}} e^{-i\frac{\psi}{n}}$ er løsning til ligningen $w^n = 1$, som vi netop har behandlet. At z opfylder $z^n = a$ er altså ensbetydende med, at z opfylder

$$\frac{z}{|a|^{1/n}} e^{-i\frac{\psi}{n}} = e^{ip\frac{2\pi}{n}} \quad \text{for passende } p \in \mathbb{Z}$$

altså at

$$z = |a|^{\frac{1}{n}} e^{i\frac{\psi}{n}} e^{ip\frac{2\pi}{n}}, \quad p \in \{o,1,\ldots n-1\}.$$

Det betyder, at <u>ligningen $z^n = a$, $a = |a|e^{i\psi}$, har de n forskellige rødder</u>

$$z = |a|^{\frac{1}{n}} e^{i\frac{\psi}{n}} z_p, \quad p \in \{o,1,\ldots n-1\}.$$

Vi skal nu se lidt nærmere på andre komplekse polynomier. Ved et komplekst <u>polynomium</u> af n'te grad forstår vi, naturligt nok, en afbildning $p: \mathbb{C} \sim \mathbb{C}$, defineret ved formen

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_o, \text{ hvor } a_o, a_1, \ldots a_n \in \mathbb{C},\ n \in \mathbb{N}$$

og hvor $a_n \neq o$. Der gælder nu, at hvis et polynomium af denne form er nul for alle $z \neq o$, så også for $z = o$. Dette følger af et simpelt kontinuitetsargument. Ved hjælp heraf slutter vi, at hvis $p(z) = o$ for alle z, så vil $a_n = a_{n-1} = \ldots a_1 = a_o$. Dette sker ved induktion. Påstanden er tydeligvis sand for n =o og for n = 1. Er den sand for n = k, så også for n = k+1. Er nemlig $p(z) = a_{k+1} z^{k+1} + \ldots a_1 z + a_o = o$ for alle $z \in \mathbb{C}$, er $a_o = o$. Da $z(a_{k+1} z^k + \ldots + a_1) = o$ for alle $z \in \mathbb{C}$, må $a_{k+1} z^k + \ldots + a_1 = o$ for alle $z \neq o$. Men så er dette k'te grads polynomium også o for $z = o$. I følge induktionsantagelsen er derfor alle $a_{k+1}, \ldots a_1 = o$. Men så er alle koefficienterne i p lig o, og påstanden bevist.

Det viser sig nu, at <u>ethvert kompleks polynomium har en rod</u>. Dette er den berømte <u>algebraens fundamentalsætning</u>. Vi vil afstå fra at bevise den her. Det er ganske vist - f.eks. med det såkaldte Argand's bevis - gennemførligt inden for den valgte ramme, suppleret med nogle let erhvervede tilføjelser, men i alt består forehavendet af så mange detaljer, at det i alt bliver for langstrakt for denne fremstilling. I det følgende skal

vi drage nogle konsekvenser af algebraens fundamentalsætning. Med den som udgangspunkt kan vi bevise

Sætning V.5. (i) Lad p være et komplekst polynomium af n'te grad, hvori c er rod. Så findes netop ét komplekst polynomium q af n-1'te grad, så at

$$(11)\quad p(z) = (z-c)q(z),\ z \in \mathbb{C}$$

(ii) Ethvert komplekst polynomium $p(z) = a_n z^n+\ldots+a_1 z+a_o$ ($a_n \neq o$) kan på netop én måde (på nær rækkefølgen) fremstilles på formen

$$(12)\quad p(z) = a_n(z-c_1)^{k_1}(z-c_2)^{k_2}\ldots(z-c_r)^{k_r},\ z \in \mathbb{C},$$

hvor $c_1,\ldots c_r$ er de indbyrdes forskellige rødder i p, og hvor $k_1,\ldots k_r \in \mathbb{N}$ med $k_1+\ldots+k_r = n$. Tallene $k_1,\ldots k_r$ kaldes røddernes **muliplicitet**er.

(iii) Ethvert komplekst polynomium har netop n rødder regnet med multipliciteter.

Bevis:

Først skal vi vise (i): Ved simpel udregning ses, at for alle $k = 1,\ldots n$ gælder:

$$z^k-c^k = (z-c)(z^{k-1}+z^{k-2}c+\ldots+zc^{k-2}+c^{k-1})$$

(højresiden er jo lig $z^k+z^{k-1}c+\ldots+zc^{k-1}-cz^{k-1}-\ldots-c^{k-1}z-c^k$). Vi sætter $q_k(z) = z^{k-1}+z^{k-2}c+\ldots+zc^{k-2}+c^{k-1}$, der er et polynomium af k-1'te grad. Derved bliver - da $p(c) = o$ -

$$p(z) = p(z) - p(o) = \sum_{k=1}^{n} a_k(z^k-c^k) = \sum_{k=1}^{n} a_k(z-c)q_k(z) =$$

$$(z-c)\sum_{k=1}^{n} a_k q_k(z).$$

Da $q(z) = \sum_{k=1}^{n} a_k q_k(z)$ er af n-1'te grad (denne grad realiseres netop af polynomiet q_n) er q et polynomium af den ønskede art. At der ikke findes andre, f.eks. r, ses af at

$$r(z) = (z-c)^{-1}p(z) = q(z)$$

for alle $z \in \mathbb{C}$, $z \neq o$. Når r og q stemmer overens for alle $z \neq o$ så også for $z = o$. Dermed er (i) vist.

Det er en umiddelbar følge af (i), at et komplekst n'te grads polynomium højst har n rødder.

Det intuitive i sagen kan forklares lidt simplere, når vi ikke skal være helt stringente i detaljerne (betegnelserne nedenfor er nogle andre end i beviset overfor). Når $p(z) = (z-r)q(z)$ og q har graden n-1, har q (hvis n-1 $\geq$ 1) en rod r_1 i følge algebraens fundamentalsætning. Så kan efter (i) q skrives på formen $q(z) = (z-r_1)q_1(z)$, hvor q har graden n-2. Hvis n-2 $\geq$ 1 kan vi fortsætte. For hver grad p har kan vi fraspalte en faktor $z-r_i$ af p, indtil vi når $(z-r_{n-1})\cdot$konst. . Det er ikke givet at $r,r_1,\ldots r_{n-1}$ er forskellige. Antallet af gange r_i forekommer er multiplicitéten af r_i. Det er for at give en stringent behandling af denne side af sagen, at vi har valgt det lidt mere knirkende induktionsbevis, som dog er bygget over den netop beskrevne tankegang.

Dette indses ved induktion efter n. For n = 1 er påstanden sand, thi $p(z) = a_1z+a_o = a_1(z+\frac{a_o}{a_1})$ har netop roden $z = -\frac{a_o}{a_1}$. Er den sand for alle polynomier af n'te grad så også for alle af n+1'te grad. Thi er p et sådant polynomium, og er c rod i p, må $p(z) = (z-c)q(z)$ efter (i). Da derved enhver rod i p må være enten c eller en rod i q, og da q har højst n rødder efter induktionsantagelsen, har p højst n+1 rødder.

Også (ii) bevises ved induktion. Påstanden er sand for n = 1, da $p(z) = a_1(z+\frac{a_o}{a_1}) = a_1(z-c_1)^1$ for $c_1 = -\frac{a_o}{a_1}$, $k_1 = 1$. Lad os dernæst antage at den er sand for alle polynomier af grad n, og lad p have graden n+1. På grund af algebraens fundamentalsætning har p en rod c, og på grund ad (i) gælder, at

$$p(z) = (z-c)q(z),$$

for et polynomium q af n'te grad, med højestegradskoefficient b_n. Efter induktionsforudsætningen findes så s indbyrdes forskellige $c_1',\ldots c_s' \in \mathbb{C}$, og $l_1,\ldots l_s \in \mathbb{N}$ med $l_1+\ldots l_s = n$, så at

$$q(z) = b_n(z-c_1')^{l_1}(z-c_2')^{l_2}\ldots((z-c_s')^{l_s}.$$

Nu må enten $c \in \{c_1',\ldots c_s'\}$ eller $c \notin \{c_1',\ldots c_s'\}$.

I det første tilfælde vil $c = c_j'$ for et $j \in \{1,\ldots s\}$. Det bevirker, at

$$p(z) = (z-c)q(z) = b_n(z-c_1')^{l_1}\ldots(z-c_j')^{l_j+1}\ldots(z-c_s')^{l_s}$$

hvor $l_1+\ldots+(l_j+1)+\ldots+l_s = n+1$. Med $r = s$, $(c_1,\ldots c_r) = (c_1'\ldots c_s')$ og $(k_1,\ldots k_j,\ldots k_r) = (l_1,\ldots l_j+1,\ldots l_s)$ har så p en fremstilling

$$p(z) = b_n(z-c_1)^{k_1}(z-c_2)^{k_2}\ldots(z-c_r)^{k_r}.$$

I det andet tilfælde har vi

$$p(z) = (z-c)q(z) = b_n(z-c)(z-c_1')^{l_1}\ldots(z-c_s')^{l_s},$$

hvor $1+l_1+\ldots+l_s = n+1$. Med $r = 1+s$, $c_1 = c$, $c_2 = c_1',\ldots c_r = c_s'$, og $k_1 = 1$, $k_2 = l_1,\ldots k_r = l_s$ har p også her en fremstilling som ovenfor.

Da koefficienten til højestegradsleddet på højre side er b_n, og på venstre side - i p - er a_n, er $a_n = b_n$. Hermed er (12)

Nok engang burde vi have givet et induktionsbevis. ⟶

(eksistensdelen) vist. Entydigheden kommer om lidt. Først konstaterer vi, at alle $c_1,...c_r$ er rødder i p. Omvendt er $p(z) = o$ netop hvis $z-c_j = o$ for et $j = 1,...r$. Det viser at rødderne i p netop udgøres af $c_1,...c_r$. Heraf følger også entydigheden af fremstillingen (12). For hvis

$$p(z) = a_n(z-d_1)^{m_1}....(z-d_t)^{m_t}$$

var en anden fremstilling af den foreskrevne art, måtte $d_1,,,d_t$ være de r rødder $c_1...c_r$, så at

$$p(z) = a_n(z-c_1)^{m_1}...(z-c_r)^{m_r}.$$

Der må så gælde, at $m_1 = k_1$. Var nemlig f.eks. $m_1 > k_1$ ville

$$a_n(z-c_1)^{m_1-k_1}(z-c_2)^{m_2}...(z-c_r)^{m_r} = a_n(z-c_2)^{k_2}\ ...(z-c_r)^{k_r}.$$

Men venstresiden har roden c_1 hvad højresiden ikke har. Dette er jo ikke muligt. Umuligheden fulgte af antagelsen om at $m_1 \neq k_1$. Derefter vises på tilsvarende måde, at $m_2 = k_2$, osv. Vi konkluderer, at de to fremstillinger er ens. Det var (ii).

Udsagent (iii) er blot en anden formulering af at summen af røddernes multipliciteter er n.

Dermed er sætningen bevist.

Der kan være grund til at se lidt nærmere på polynomier, hvor alle koefficienter er reelle. Lad p være et sådant polynomium. Først gør vi den observation, at $p(\bar{z}) = \overline{p(z)}$. Det følger af, at

$$p(z) = a_n\bar{z}^n+...+a_1\bar{z}+a_o = a_n\overline{z^n}+...+a_1\bar{z}+a_o = \bar{a}_n\overline{z^n}+...+\bar{a}_1\bar{z}+\bar{a}_o = \overline{p(z)}$$

hvor vi har benyttet, at konjugering er en homomorfi og at $\bar{a}_k = a_k$ når a_k er reel.

Af $p(\bar{z}) = \overline{p(z)}$ følger, at hvis c er rod i p så er også $\bar{c}$ rod. Thi $p(\bar{c}) = \overline{p(o)} = \bar{o} = o$. Er c egentligt kompleks, har c og $\bar{c}$ samme multipliciteter. Var disse nemlig, hhv. k og m, forskellige, havde p fremstillingen (i kraft af (12))

$$p(z) = (z-c)^k(z-\bar{c})^m\ q(z),$$

hvor q hverken har c eller $\bar{c}$ som rod. Var nu $k < m$ (hvis den omvendte ulighed holdt argumenterede vi tilsvarende), ville vi have

Der er ikke nogen differentiationsproces involveret!

Gennemfør selv denne sammenholdning. Det er let, men detaljerigt.

De indgående 2.grads polynomier har selvfølgelig ingen reelle rødder (så havde p haft flere sådanne end $c_1,\ldots c_s$). Det stemmer hermed, at diskriminanterne er negative:
$(d_j+\bar{d}_j)^2-4d_j\bar{d}_j = d_j^2+\bar{d}_j^2+2d_j\bar{d}_j-4d_j\bar{d}_j = (d_j-\bar{d}_j)^2 = (2i\mathrm{Im}(d_j))^2$
$= -4(\mathrm{Im}(d_j))^2 < 0.$

$$p(z) = (z-c)^k(z-\bar{c})^k(z-\bar{c})^{m-k}q(z).$$

Nu er $(z-c)(z-\bar{c}) = z^2-(c+\bar{c})z+c\bar{c}$, og da $c+\bar{c}$ og $c\bar{c} = |c|^2$ begge er reelle har dette 2.grads polynomium altså reelle koefficienter. Vi kan skrive det z^2-rz+s. Nu må

$$\frac{p(z)}{z^2-rz+s} = p'(z)$$

være et polynomium med reelle koefficienter. At det er et polynomium ses af, at $p'(z) = (z-c)^{m-k}(z^2-rz+s)^{k-1}q(z)$. At koefficienterne er reelle ses ved parvis sammenholdning af dem i $p(z)$ og $p'(z)(z^2-rz+s)$. Ved anvendelse af dette ræsonnement k gange finder vi, at polynomiet $(z-c)^{m-k}q(z)$ har reelle koefficienter. Det har tydeligvis roden c. Derfor må det også have $\bar{c}$ som rod. Da c er egentligt kompleks må $\bar{c}$ være rod i q. Men q har ikke $\bar{c}$ som rod. Altså kan m og k ikke være forskellige.

Af disse betragtninger følger, at de egentligt komplekse rødder i et polynomium med reelle koefficienter falder i <u>par af konjugerede med samme multiplicitet</u>. Det bevirker, at faktoriseringen af et sådant polynomium p efter Sætning V.5. antager skikkelsen

$$p(z) = a_n(z-c_1)^{k_1}\ldots(z-c_s)^{k_s}(z-d_1)^{j_1}(z-\bar{d}_1)^{j_1}\ldots(z-d_t)^{j_t}(z-\bar{d}_t)^{j_t}$$

hvor $c_1,\ldots c_s$ er de reelle rødder, $d_1,\ldots d_t$ de egentligt komplekse rødder med deres konjugerede $\bar{d}_1,\ldots\bar{d}_t$, og hvor $k_1+\cdots+k_s+2j_1+..+2j_t = n$. Heraf fås vi uden videre en <u>faktorisering af p i lutter reelle polynomier</u>:

$$p(z) = a_n(z-c_1)^{k_1}\ldots(z-c_s)^{k_s}(z^2-(d_1+\bar{d}_1)z+d_1\bar{d}_1)^{j_1}$$
$$\ldots(z^2-(d_t+\bar{d}_t)z+d_t\bar{d}_t)^{j_t},$$

hvor alle $d_1+\bar{d}_1,\ldots d_t+\bar{d}_t$ og $d_1\bar{d}_1,\ldots d_t\bar{d}_t$ er reelle.

<u>De komplekse tals kardinalitet</u>

Dette spørgsmål er hurtigt overstået, al den stund de komplekse tal jo simpelthen er elementerne i $\mathbb{R}^2$ (blot organiseret i en særlig algebraisk struktur). Da $\mathbb{R}^2$ er ækvipotent med $\mathbb{R}$, er dermed <u>$\mathbb{C}$ ækvipotent med $\mathbb{R}$</u>.

ALGEBRAISKE FORBEREDELSER

Vi skal i denne tekst beskæftige os med at etablere et udvalg af begreber og resultater om algebraiske strukturer. Emnevalget skal ikke forestille at udgøre en udtømmende præsentation af teorien for algebraiske strukturer. Det skal kun tjene som basis for udvidelsen af de naturlige tal til de hele tal, af disse igen til de rationale osv. Selv om fremstillingen ikke er udtømmende,er den dog tilstræbt at være konsistent og hulfri. Den skulle kunne læses på basis af minimale forudsætninger, kun omfattende logik og simpel mængdelære, inklusive elementær afbildningsteori.

Vi lægger ud med

0. Præ-algebraiske forberedelser. Relationer.

Et af de grundlæggende begreber i matematikken er begrebet relation. Som eksempler på relationer kan vi nævne "=" (lig med), "<" (mindre end), "$\subseteq$" (delmængde af) og "|"(gå op i).

Lad A og B være mængder. Løst sagt forestiller vi os nu, at den relation vi tænker på fastlægges ved at det afgøres om et givet $a \in A$ og et givet $b \in B$ står i relation til hinanden. Nærmere bestemt kommer dette ud på at udpege de par $(a,b) \in AxB$, der skal stå i relation til hinanden, hvilket er det samme som at udpege den delmængde af AxB, som udgøres af de pågældende par. Præcist:

Definition 0.1. En relation fra en mængde A til en mængde B er den delmængde, R, af AxB. Hvis A = B, taler vi om en relation i A.

Vi interesserer os her kun for relationer i en mængde A, og i virkeligheden især for to typer af relationer, som fastlægges lidt senere. Først indføres yderligere nogle begreber.

Definition 0.2 En relation R i en mængde A siges at være

refleksiv, hvis: $\forall x \in A: (x,x) \in R$,
irrefleksiv, hvis: $\forall x \in A: (x,x) \notin R$,
symmetrisk, hvis: $\forall x,y \in A: (x,y) \in R \Rightarrow (y,x) \in R$
asymmetrisk, hvis $\forall x,y \in A: (x,y) \in R \Rightarrow (y,x) \notin R$
antisymmetrisk, hvis $\forall x,y \in A: (x,y) \in R$ og $(y,x) \in R \Rightarrow x = y$
transitiv, hvis $\forall x,y,z \in A: (x,y) \in R$ og $(y,z) \in R \Rightarrow (x,z) \in R$

Definition 0.3. Ved en irrefleksiv ordningsrelation i en mængde A forstås en relation, der er irrefleksiv, asymmetrisk og transitiv. Ved en refleksiv ordningsrelation i A forstås en relation, der er refleksiv, antisymmetrisk og transitiv.

Standardeksemplet på en irrefleksiv ordningsrelation er "<" (eller ">"). Et andet eksempel er "$\subset$" (eller "$\supset$"). Standardeksemplet på en refleksiv ordningsrelation er "$\leq$" (eller "$\geq$"). Et andet eksempel er "$\subseteq$" (eller "$\supseteq$").

Hvis R er en irrefleksiv ordningsrelation kan vi ved tilføjelse af diagonalen $\{(x,x) \in AxA \mid x \in A\}$ opnå den tilsvarende refleksive ordningsrelation $R \cup \{(x,x) \in AxA \mid x \in A\}$. Omvendt kan vi ved fjernelse af diagonalen fra en refleksiv ordningsrelation opnå den tilsvarende irrefleksive $R \setminus \{(x,x) \in AxA \mid x \in A\}$. Det er en simpel checkopgave at kontrollere, at de to relationer faktisk er af den påståede type.

Definition 0.4. Ved en ækvivalensrelation i en mængde A forstås en relation, der er refleksiv, symmetrisk og transitiv.

Standardeksemplet på en ækvivalensrelation er identitetsrelationen "=". En generel ækvivalensrelation betegnes ofte med $\sim$.

Resten af afsnittet vil blive viet ækvivalensrelationer og deres pårørende.

Har vi at gøre med en ækvivalensrelation $\sim$ i A betegnes med G_a klassen af elementer, der er ækvivalente med a (dvs. står i ækvivalensrelationen til a):

$$G_a = \{x \in A \mid x \sim a\} .$$

Det er oplagt, at $a \in G_a$, da $a \sim a$, på grund af refleksiviteten.

Hvis $a \sim b$, er $G_a = G_b$. Thi hvis $x \in G_a$, vil $x \sim a$, og da $a \sim b$, vil også $x \sim b$ (transitiviteten), hvorved $x \in G_b$. Så er $G_a \subseteq G_b$. På helt tilsvarende måde ses, at $G_b \subseteq G_a$. Så er påstanden bevist.

Hvis a og b er vilkårlige elementer i A gælder, at enten er G_a og G_b identiske (nemlig hvis $a \sim b$), eller også har de ingen elementer fælles, dvs. enten er $G_a = G_b$ eller $G_a \cap G_b = \emptyset$.

Dette indses på følgende måde:

Lad os antage, at G_a og G_b har mindst ét element fælles: $x \in G_a \cap G_b$. Så må $x \sim a$ og $x \sim b$, og dermed (p.g.a. symmetrien og transitiviteten) $a \sim b$. Men så er i følge det foregående $G_a = G_b$.

På denne baggrund er det rimeligt at omtale G_a som ækvivalensklassen indeholdende a, idet der findes én og kun én klasse af formen G_a, der indeholder a. Ethvert element i en ækvivalensklasse kaldes en repræsentant for den.

Betragtes nu samlingen $\{G_a \mid a \in A\}$ af alle ækvivalensklasser, ses at

$$A = \bigcup_{a \in A} G_a \quad (= \{x \in A \mid \exists a \in A: x \in G_a\})$$
$$\text{def.}$$

thi: Hvis $x \in A$, vil nemlig $x \in G_x$ og dermed $x \in \bigcup\{G_a \mid a \in A\}$. Da elle elementeri $\bigcup\{G_a \mid a \in A\}$pr. definition ligger i A, ses det, at $\bigcup G_a \subseteq A$. Således har vi vist, at både $A \subseteq \bigcup G_a$ og, at $\bigcup G_a \subseteq A$.

Vi har altså indset, at samlingen af alle G_a'er tilsammen udfylder hele A med ikke-tomme mængder, og at de er indbyrdes dis-

junkte (to og to ikke har nogen elementer fælles). Det er i familje med et generelt fænomen:

Definition 0.5. Lad A være en vilkårlig mængde. Ved en klassedeling af A (eller en partition af A) forstås en samling af delmængder af A:

$\{K_\alpha \mid \alpha \in I\}$,

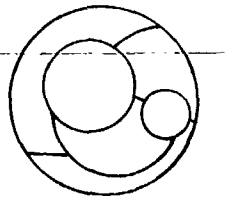
der opfylder

(1) $\forall \alpha \in I: K_\alpha \neq \emptyset$

(2) $\forall \alpha, \beta \in I: K_\alpha = K_\beta$ eller $K_\alpha \cap K_\beta = \emptyset$

og

(3) $\bigcup_{\alpha \in I} K_\alpha = A$.



De ovenstående betragninger vedrørende ækvivalensklasser gør at vi har bevist:

Sætning 0.6. Hvis ~ er en ækvivalensrelation i en mængde A, udgør ækvivalensklasserne en klassedeling af A.

Nu kan man spørge, om enhver klassedeling kan realiseres som den til en eller anden ækvivalensrelation svarende klassedeling bestående af ækvivalensklasserne. Svaret er bekræftende, og der findes endda kun én sådan ækvivalensrelation:

Sætning 0.7. Hvis $\{K_\alpha \mid \alpha \in I\}$ er en klassedeling af A, findes én (og kun én) ækvivalensrelation ~, hvis ækvivalensklasser netop er $\{K_\alpha \mid \alpha \in I\}$.

Bevis: Eksistensdelen først.

Det er nærliggende at forsøge med følgende definition af ~:

a ~ b hvis og kun hvis der findes en klasse K_α, så at $a \in K_\alpha$ og $b \in K_\alpha$.

At ~ med denne definition virkelig bliver en ækvivalensrelation ses således: Refleksiviteten følger af, at da a tilhører en klasse K_α (p.g.a. (3)), gælder $a \in K_\alpha$, og $a \in K_\alpha$, dvs. $a \sim a$. Hvad symmetrien angår har vi: Hvis $a \sim b$, findes en klasse K_α, så at $a \in K_\alpha$, og $b \in K_\alpha$. Da $a \in K_\alpha$ og $b \in K_\alpha$ er det samme som, at $b \in K_\alpha$ og $a \in K_\alpha$, har vi $b \sim a$. Altså er ~ symmetrisk. Endelig transitiviteten: Hvis $a \sim b$ og $b \sim c$, findes K_α og K_β, så at $a \in K_\alpha$ og $b \in K_\alpha$, såvel som $b \in K_\beta$ og $c \in K_\beta$. Det fører til, at $b \in K_\alpha \cap K_\beta$. I kraft af (2) må så $K_\alpha = K_\beta$, hvorved $a, b, c \in K_\alpha$. Specielt vil $a \in K_\alpha$ og $c \in K_\alpha$, så at $a \sim c$.

Derved har vi skaffet en ækvivalensrelation ~. Vi skylder blot at vise, at samlingen af dens ækvivalensklasser $\{G_a \mid a \in A\}$ netop er $\{K_\alpha \mid \alpha \in I\}$.

Lad til den ende G_a være en vilkårlig ækvivalensklasse. Da K_α'erne udgør en klassedeling, findes netop én klasse K_α, så at $a \in K_\alpha$. Så er $G_a = K_\alpha$. Thi, hvis $b \in G_a$, er $b \sim a$, hvorved a og b tilhøre samme K-klasse. Da $a \in K_\alpha$, må denne være K_α. Altså vil $b \in K_\alpha$ og dermed $G_a \subseteq K$. Hvis omvendt $b \in K_\alpha$, vil, da $a \in K_\alpha$ a og b tilhøre samme klasse K. Så er $a \sim b$ og $b \in G_a$. Det viser, at $K \subseteq G_a$, så at vi i alt har $G_a = K_\alpha$.

Dermed har vi godtgjort, at enhver ækvivalensklasse findes blandt K-erne. Det omvendte er imidlertid også tilfældet. Lad nemlig K være en vilkårlig klasse fra $\{K_\alpha \mid \alpha \in I\}$, og lad a være et vilkårligt element i K_α (et sådant findes p.g.a. (1)). Så er $G_a = K$ med helt det samme argument som før.

Hermed er eksistensdelen bevist.

Entydighedsdelen følger således: Lad os antage, at der eksisterede to ækvivalensrelationer ~ og ≈, hvis ækvivalensklassesystemer begge stemte overens med K_α $\alpha \in I$. Så måtte:

$\{\tilde{G}_a \mid a \in A\} = \{\tilde{\tilde{G}}_a \mid a \in A\}$

Vi skal vise, at $a \sim b$ er ensbetydende med, at $a \approx b$. Lad først $a \sim b$, dvs. $a \in \tilde{G}_b$. Nu findes i kraft af identiteten ovenfor et $b' \in A$, så at $\tilde{G}_b = \tilde{\tilde{G}}_{b'}$. Så vil $a \in \tilde{\tilde{G}}_{b'}$, og da også $b \in \tilde{G}_b = \tilde{\tilde{G}}_{b'}$, tilhører a og b samme ≈-klasse. Men så er $a \approx b$. På aldeles samme måde indses, at hvis $a \approx b$, vil $a \sim b$. Q.E.D.

Sætning 0.6. og 0.7 siger, at ækvivalensrelationerne og klassedelinger er to sider af samme sag. Man har specificeret det ene, når man har det andet.

Definition 0.8. Hvis A er en mængde og ~ en ækvivalensrelation i A kaldes den mængde, hvis elementer er ækvivalensklasserne for kvotientmængden. Den betegnes A/~.

Intuitivt er der ved betragning af kvotientmængden tale om, at man ser bort fra forskellene mellem ækvivalente elementer. Ækvivalensrelationen udtrykker nærmest, at i en bestemt henseende er ækvivalente elementer at regne for ens. De interessante forskelle mellem elementerne løftes dermed op og repræsenteres som forskelle mellem ækvivalensklasserne.

Definition 0.9 Hvis ~ er en ækvivalensrelation i en mængde A, kaldes afbildningen $\varphi: x \sim G_x$, fra A ind i A/~ for den kanoniske afbildning.

Idet enhver ækvivalensklasse i A/~ er billede af ethvert af sine elementer (og der findes altid mindst ét sådant på grund af (1)), er den kanoniske afbildning altid surjektiv. Den er derimod normalt ikke injektiv. Det sker kun i det trivielle tilfælde, hvor ækvivalensrelationen er lig identiteten.

I. Organiserede mængder

Det er overordentlig hyppigt forekommende i matematikken at betragte en mængde forsynet med en komposition, dvs. en forskrift, der til to vilkårlige elementer i mængden knytter et tredje.

I den formelle ramme, vi betragter, tager dette sig således ud:

Definition I.1. Ved en komposition i en mængde A forstås en afbildning fra AxA ind i A.

Hvis f er en komposition i A, skulle billedet ved f af (a,b) normalt angives f(a,b). Denne skrivemåde er imidlertid ubekvem. Dels fordi den ikke er gængs i litteraturen, dels fordi den ikke er intuitivt appellerende. Man ser i stedet oftest kompositioner betegnet med symboler, der skal minde om konkrete kompositioner fra hverdagen x,·,∩,∪osv., f.eks. ⁰, $, §, †. Lad os som typisk symbol for en komposition bruge tegnet "§". I stedet for at skrive §(a,b) skriver vi (og man) a§b. Dette er altså et rent notationsmæssigt anliggende.

Hvis § er en komposition i en mængde A, siger vi, at A er organiseret ved kompositionen §. Vi skriver (A,§) og taler om elementerne i A som elementer i (A,§).

Det forekommer ofte, at man beskæftiger sig med mængder i hvilke der samtidig er givet mere end én komposition. Vi nævner her følgende generelle definition:

Definition I.2. Ved en algebraisk struktur eller en organiseret mængde forstås en mængde, i hvilken der er givet et endeligt antal kompositioner. Hvis mængden hedder A og kompositionerne $\S_1, \S_2, \ldots, \S_n$, skriver vi $(A, \S_1, \S_2, \ldots \S_n)$.

II . Mængder med én komposition.

I dette afsnit vil vi se på mængder, i hvilke der kun er givet én komposition. Vi starter med en række definitioner:

Definition II.1. En komposition § i en mængde A kaldes associativ, hvis (og kun hvis)

(1) $\forall a,b,c \in A: (a\S b)\S c = a\S(b\S c)$.

Definition II.2. En komposition § i en mængde A kaldes kommutativ, hvis (og kun hvis)

(2) $\forall\, a,b \in A: a\S b = b\S a$.

Definition II.3. Et element ν i en organiseret mængde (A,§) kaldes et neutralt element ved §, hvis (og kun hvis)

(3) $\forall a \in A: a\S\nu = \nu\S a = a$

Sætning II.4. Hvis § er en komposition i A, findes højst ét neutralt element ved § i A.

Bevis. Antog vi, at ν_1 og ν_2 begge var neutrale elementer ved §, måtte der gælde

$\nu_1\S\nu_2 = \nu_2\S\nu_1 = \nu_1$ ((3) med ν_1 som a og ν_2 som ν)

og

$\nu_2\S\nu_1 = \nu_1\S\nu_2 = \nu_2$ ((3) med ν_2 som a og ν_1 som ν),

hvoraf

$\nu_1 = \nu_2$,

hvilket skulle bevises.

Bemærkning. Sætning II.4 lover intet om, at der overhovedet findes noget neutralt element i (A,§), kun at der i givet fald højst findes ét.

Definition II.5. Lad der i (A,§) være et neutralt element ν. Et element a i A kaldes invertibelt, hvis der findes et element b i A, så at

(4) $a\S b = b\S a = \nu$.

Hvis (4) er opfyldt, kaldes b et inverst element til a.

Sætning II.6. Hvis (A,§) er associativ, findes der til hvert a i A højst ét inverst element.

Bevis. Antog vi, at b_1 og b_2 opfyldte

$a\S b_1 = b_1\S a = \nu$

og

$a\S b_2 = b_2\S a = \nu$,

måtte

$$b_1 = b_1 \S \nu = b_1 \S (a \S b_2) = (b_1 \S a) \S b_2 = \nu \S b_2 = b_2,$$

hvorved beviset er fuldført.

Bemærkning. Sætning II.6 lover ikke, at der til et givet a overhovedet findes et inverst.

Det faktum, at der til et givet a i (A,§) (med § associativ) højst findes ét b, så at (4) er opfyldt, gør det rimeligt for et invertibelt element i (A,§) at tale ikke blot om "et inverst element" til a, men om "det inverse element" til a. Det inverse element til a betegnes a^{-1}. Vi kan altså formulere (4) som

$$a \S a^{-1} = a^{-1} \S a = \nu.$$

Det ses, at a er det inverse til a^{-1}, altså at $(a^{-1})^{-1} = a$.

Definition II.7. Hvis § er en komposition i A, siges forkortningsreglerne at gælde i (A,§), såfremt

(5) $\forall\, a,b,x \in A$: $a \S x = b \S x \Rightarrow a = b$

og

(6) $\forall\, a,b,x \in A$: $x \S a = x \S b \Rightarrow a = b$.

Definition II.8. Ved en halvgruppe eller en semigruppe forstås en organiseret mængde (A,§), hvor § er associativ og hvori forkortningsreglerne gælder.

Definition II.9. Ved en gruppe forstås en organiseret mængde (A,§) således, at

(7) G1: § er associativ
(8) G2: der findes et neutralt element i (A,§)
(9) G3: ethvert element i (A,§) er invertibelt.

Definition II.lo. Ved en abelsk eller en kommutativ gruppe forstås en gruppe, hvori kompositionen er kommutativ.

Nu ville det være lidt sært, hvis der kunne tænkes grupper, der ikke også var halvgrupper. Dette forhindres af:

Sætning II.11. I en gruppe gælder forkortningsreglerne.

Bevis. Lad gruppen hedde (A,§), og lad a,b,x være vilkårlige elementer i A, så at

$$a \S x = b \S x.$$

Da A er en gruppe, har ethvert element - og derfor også x - et inverst. Vi har så, at

$$a = a \S \nu = a \S (x \S x^{-1}) = (a \S x) \S x^{-1} = (b \S x) \S x^{-1} = b \S (x \S x^{-1}) = b \S \nu = b.$$

Da altså a = b, er (5) bevist. Beviset for (6) forløber helt parallelt. Q.E.D.

Vi kan udtrykke den bortvejrede særhed således:

Sætning II.12. Enhver gruppe er en halvgruppe.

Bevis. Trivielt i kraft af sætning II.11.

Hvis § er en komposition i A, og B er en delmængde af A, kan § under visse omstændigheder betragtes som en komposition i B, nemlig hvis

(lo) $\forall\, b_1,b_2 \in B$: $b_1 \S b_2 \in B$

I så fald vil nemlig restriktionen af § til BxB være en afbildning ind i B, hvilket tillader os at tale om den organiserede mængde (B,§).

Dette leder til

Definition II.13. Hvis (A,§) er en organiseret mængde og B er en delmængde af A, siges B at være stabil, hvis (lo) er opfyldt.

Definition II.14. Hvis (A,§) er en gruppe, og B er en stabil delmængde af A, siges (B,§) at være en undergruppe af A, hvis (B,§) er en gruppe.

Sætning II.15. Hvis (A,§) er en gruppe og B er en ikke-tom delmængde af A, gælder:

(B,§) er en undergruppe af (A,§) hvis og kun hvis

(11) B er stabil
og
(12) $\forall\, b \in B$: $b^{-1} \in B$

(Her skal b^{-1} forstås som det inverse til b i A).

Bevis.
"Kun hvis": Hvis (B,§) er en undergruppe af (A,§), må B være stabil (jvf. definition II.13). Således er (11) opfyldt. Lad dernæst b være et vilkårligt element i B. Da $(B,\S_{1(B)})$ er en gruppe, er b invertibelt i B, med det inverse $b^{-1(B)}$. Da b også er element i gruppen $(A,\S_1)$, er b endvidere invertibelt i A, med det inverse b^{-1}. Imidlertid har b jo netop ét inverst i A, hvorfor

$$b^{-1} = b^{-1(B)} \in B.$$

Altså gælder (12).
"Hvis": Lad $B \subseteq A$ opfylde (11) og (12). Det har dermed mening at betragte (B,§). Vi skal vise, at (B,§) er en gruppe.
Ad G1: Da kompositionen er associativ i A, er den også associativ i B.
Ad G2: I (A,§) findes et neutralt element, ν. Vi vil vise, at det tilhører B, hvorfor det så naturligvis må være neutralt element i B.
Da B er ikke-tom, findes et element, lad os sige b_o, i B. Da B opfylder (12), vil også $b_o^{-1} \in B$. I kraft af B's stabilitet vil dermed

$$\nu = b_o \S b_o^{-1} \in B.$$

Ad G3: Lad b være et vilkårligt element i B. På grund af (12) vil $b^{-1} \in B$. Men så er b^{-1} også invers til b i B, hvorved b er invertibelt i B. Dermed er (B,§) en gruppe, og sætningen er bevist.

III. Afbildninger mellem to mængder med hver én komposition

Hvis A og B er to mængder, hver forsynet med en komposition (henholdsvis § og †), er det rimeligt at undersøge, hvordan kompositionerne spiller sammen med afbildninger mellem mængderne.

Definition III.1. Lad (A,§) og (B,†) være givne og lad f:A→B være en afbildning. Så kaldes f en homomorfi fra (A,§) til (B,†), hvis

(13) $\forall a_1,a_2 \in A: f(a_1 \S a_2) = f(a_1) \dagger f(a_2)$.

Definition III.2. Hvis f er en homomorfi fra (A,§) til (B,†) og tillige er bijektiv, kaldes f en isomorfi.

Sætning III.3. Hvis f er en isomorfi fra (A,§) til (B,†) er f^{-1} (der er veldefineret fordi f er bijektiv) en isomorfi fra (B,†) til (A,§).

Bevis. Lad b_1 og b_2 være vilkårlige elementer i B. Sættes

$$a_1 = f^{-1}(b_1) \text{ og } a_2 = f^{-1}(b_2)$$

gælder, da f er en homomorfi, at

$$f(a_1 \S a_2) = f(a_1) \dagger f(a_2) = f(f^{-1}(b_1)) \dagger f(f^{-1}(b_2))$$
$$= I_B(b_1) \dagger I_B(b_2) = b_1 \dagger b_2.$$

Men så vil

$$f^{-1}(b_1 \dagger b_2) = f^{-1}(f(a_1 \S a_2)) = I_A(a_1 \S a_2) = a_1 \S a_2$$
$$= f^{-1}(b_1) \S f^{-1}(b_2),$$

hvilket viser, at f^{-1} er en homomorfi fra (B,†) til (A,§). Da vi endvidere ved, at f^{-1} er bijektiv, er sætningen bevist.

I hvor høj grad overføres egenskaber ved § til † ved en homomorfi fra (A,§) til (B,†)?

Sætning III.4. Laf f:A→B være en surjektiv homomorfi fra (A,§) til (B,†). Så gælder

(a) Hvis § er associativ er også † associativ.
(b) Hvis § er kommutativ er også † kommutativ.
(c) Hvis der findes et neutralt element i (A,§), findes der også et neutralt element i (B,†). Hvis tillige a er invertibel i (A,§) er f(a) invertibel i (B,†). Er ydermere § associativ, er
$(f(a))^{-1} = f(a^{-1})$.
(d) Hvis (A,§) har et neutralt element, og hvis ethvert element i (A,§) er invertibelt, er også ethvert element i (B,†) invertibelt.

Bevis.

(a) Vi antager, at § er associativ. Lad b_1,b_2,b_3 være vilkårlige elementer i B. Da f er surjektiv, findes a_1,a_2,a_3 i A, så at

$$f(a_1) = b_1,\ f(a_2) = b_2,\ f(a_3) = b_3.$$

Nu vil

$$(b_1 \dagger b_2) \dagger b_3 = (f(a_1) \dagger f(a_2)) \dagger f(a_3) = f(a_1 \S a_2) \dagger f(a_3)$$
$$= f((a_1 \S a_2) \S a_3) = f(a_1 \S (a_2 \S a_3))$$
$$= f(a_1) \dagger f(a_2 \dagger a_3) = f(a_1) \dagger (f(a_2) \dagger f(a_3))$$
$$= b_1 \dagger (b_2 \dagger b_3),$$

hvor det 2.,3.,5., og 6. lighedstegn følger af, at f er en homomorfi.

(b) Bevises analogt til (a). Prøv selv.

(c) Lad ν være neutralt element i (A,§). Så vil f(ν) være neutralt element i (B,†). Lad nemlig b være et vilkårligt element i B. Så findes, da f er surjektiv, et a i A, så at f(a) = b. Da

$$b \dagger f(\nu) = f(a) \dagger f(\nu) = f(a \S \nu) = f(a) = b,$$

og

$$f(\nu) \dagger b = f(\nu) \dagger f(a) = f(\nu \S a) = f(a) = b,$$

er påstanden bevist.

Hvis yderligere a er invertibel i (A,§), er f(a) invertibel i (B,†). Lad nemlig a_1 i A opfylde

$$a \S a_1 = a_1 \S a = \nu.$$

Så vil

$$f(a_1) \dagger f(a) = f(a_1 \S a) = f(\nu)$$

og

$$f(a) \dagger f(a_1) = f(a \S a_1) = f(\nu),$$

hvilket viser, at f(a) er invertibel.

Hvis desuden § er associativ, er a_1 entydigt bestemt, og kan kaldes a^{-1}. Da også † er associativ (se (a)), vil der findes netop ét inverst til f(a), hvorfor

$$f(a^{-1}) = (f(a))^{-1}.$$

(d) Lad b være element i B. Da f er surjektiv, findes a i A, så at f(a) = b. Da ethvert element i A er invertibelt, er specielt a invertibelt. Så er i følge (c) også b (= f(a)) invertibel.

Hermed er sætningen bevist.

Sætning III.5. Hvis (A,§) er en gruppe og (B,†) en organiseret mængde, og hvis f er en surjektiv homomorfi fra (A,§) til (B,†), er også (B,†) en gruppe.

Bevis. I følge sætning III.4 (a) er †associativ, og i følge (c) har (B,†) et neutralt element. Endelig slutter vi af (d), at ethvert element i (B,†) er invertibelt. Men så er (B,†) en gruppe. Q.E.D.

For at forkortningsreglerne skal kunne overføres ved en surjektiv homomorfi, må denne tillige være injektiv, altså en isomorfi:

Sætning III.6. Hvis f er en isomorfi fra (A,§) til (B,†), og

hvis forkortningsreglerne gælder i den ene af de organiserede mængder (A,§) eller (B,†), gælder de også i den anden.

Bevis. (1) Lad os antage, at forkortningsreglerne gælder i (A,§), og lad b_1 og b_2 være vilkårlige elementer i B, så at

$$b_1 \dagger y = b_2 \dagger y.$$

Da f er surjektiv, findes a_1, a_2, x i A, så at

$$f(a_1) = b_1,\ f(a_2) = b_2,\ f(x) = y.$$

Nu vil

$$f(a_1 \S x) = f(a_1) \dagger f(x) = b_1 \dagger y = b_2 \dagger y = f(a_2) \dagger f(x) = f(a_2 \S x),$$

og da f er injektiv, må dermed

$$a_1 \S x = a_2 \S x.$$

Eftersom forkortningsreglerne gælder i (A,§), må så $a_1 = a_2$ og dermed

$$b_1 = f(a_1) = f(a_2) = b_2.$$

På tilsvarende måde vises, at hvis

$$y \dagger b_1 = y \dagger b_2,$$

må $b_1 = b_2$.

(2). Hvis forkortningsreglerne gælder i(B,†), må de også gælde i (A,§). Thi f^{-1} er en isomorfi (sætning III.3), fra (B,†) til (A,§), hvorfor vi efter en anvendelse af det netop beviste på f^{-1} slutter det ønskede.

Sætning III.7. Hvis f er en isomorfi fra (A,§) til (B,†), og hvis den ene af (A,§) eller (B,†) er en semigruppe, er også den anden en semigruppe.

Bevis. Beviset følger umiddelbart af sætning III.4. (a) og af sætning III.6.

IV. Ækvivalensrelation og komposition

Lad der være givet en organiseret mængde (A,§) og en ækvivalensrelation $\sim$ i A. Findes der en "naturlig" måde til at overføre kompositionen § i A til en komposition i mængden af ækvivalensklasser (ved $\sim$) i A?

Et umiddelbart bud ville være følgende:

Lad

$$G_a = \{x \varepsilon A \mid x \sim a\} \quad \text{og} \quad G_b = \{x \varepsilon A \mid x \sim b\}$$

være to vilkårlige ækvivalensklasser i A/$\sim$. Skulle man angive en ækvivalensklasse, der kunne tjene som den komponerede af G_a og G_b, ville det være nærliggende at pege på

$$G_{a \S b} = \{x \varepsilon A \mid x \sim a \S b\}.$$

Dette rejser imidlertid i første omgang nogle problemer. Hvis nemlig a' og b' var vilkårlige andre elementer i G_a henholdsvis G_b, ville jo

$$G_a = G_{a'} \text{ og } G_b = G_{b'}.$$

Skulle der være mening i bestræbelsen på at definere en "naturlig" komposition i A/$\sim$ på den anførte måde, måtte så også

$$G_{a' \S b'} = G_{a \S b}.$$

Disse overvejelser leder til indførelsen af følgende begreb:

Definition IV.1. Lad (A,§) være en organiseret mængde og lad $\sim$ være en ækvivalensrelation i A. Vi siger, at ækvivalensrelationen $\sim$ harmonerer med kompositionen §, hvis det for alle a_1, a_2, b_1, b_2 i A gælder, at

(14) $a_1 \sim a_2$ og $b_1 \sim b_2 \Rightarrow a_1 \S b_1 \sim a_2 \S b_2$

(Undertiden kaldes en med en komposition harmonerende ækvivalensrelation for en kongruensrelation.)

Lad os nu betragte (A,§) og en ækvivalensrelation $\sim$, der harmonerer med §. Under disse omstændigheder kan vi være sikre på, at hvis

$$G_a = G_{a'} \text{ og } G_b = G_{b''},$$

vil også

$$G_{a \S b} = G_{a' \S b''}$$

idet jo $a \sim a'$ og $b \sim b' \Rightarrow a \S b \sim a' \S b'$ og $a \S b \sim a' \S b' \Rightarrow G_{a \S b} = G_{a' \S b''}$.

Det betyder, at vi kan komponere to ækvivalensklasser ved at udtage ækvivalensklassen bestående af det komponerede element af to vilkårlige repræsentanter, én fra hver ækvivalensklasse.

Vi kan derfor tillade os at formulere

Definition IV.2. Lad (A,§) være en organiseret mængde og lad $\sim$ være en ækvivalensrelation, der harmonerer med §. Ved den inducerede komposition på kvotientmængden A/$\sim$ forstås kompositionen $\S^{\sim}$, defineret ved for vilkårlige G_1 og G_2 i A/$\sim$ at sætte (idet a er en vilkårlig repræsentant i G_1 og b en vilkårlig repræsentant i G_2):

(15) $G_1 \S^{\sim} G_2 = G_a \S^{\sim} G_b = G_{a \S b}$.

Betragter vi i denne sammenhæng den kanoniske afbildning, fra A til A/$\sim$, der jo er defineret ved

(16) $\forall\, x \varepsilon A\colon f(x) = G_x$,

kan vi indse, at egenskaberne ved § overføres til egenskaber ved $\S^{\sim}$, i kraft af

Sætning IV.3. Hvis $\sim$er en ækvivalensrelation, der harmonerer med kompositionen i den organiserede mængde (A,§), er den kanoniske afbildning fra (A,§) til (A/$\sim$,$\S^{\sim}$) en surjektiv homomorfi.

Bevis. (1) Lad os få surjektiviteten overstået først: For en vilkårlig ækvivalensklasse G i A/$\sim$ findes et a i A, så at $G = G_a$. Da så

$G = G_a = f(a)$,

er G billede ved f af et element i A.

(2) Homomorfiegenskaben er en gratis konsekvens af definitionen på $\S^{\sim}$:

$f(a\S b) = G_{a\S b} = G_a \S^{\sim} G_b = f(a)\S^{\sim} f(b)$,

hvilket skulle bevises.

Sammenholder vi dette resultat med sætningerne III.4 og III.5, ser vi, at de i dem beskrevne egenskaber ved § overføres til egenskaber ved $\S^{\sim}$.

V. Mængder med to kompositioner. Ringe og legemer

Når det gælder talsystemernes opbygning er mængder forsynet med to kompositioner de relevante matematiske objekter at studere, fordi der i alle de talsystemer vi betragter findes både en addition og en multiplikation.

Lad der derfor være givet en mængde A med to kompositioner § og $. Vi angiver, at A er organiseret ved disse to kompositioner ved at skrive (A,§,$). Oftest vil § spille rollen af "plus" og $ rollen af "gange". I denne sammenhæng studeres de dog alment. Vi lægger ud med en række definitioner.

Definition V.1 Lad (A,§,$) være en organiseret mængde. Kompositionen $ siges at være distributiv med hensyn til §, hvis både

(17) $\forall a,b,c \in A: a\$(b\S c) = (a\$b)\S(a\$c)$

og

(18) $\forall a,b,c \in A: (b\S c)\$a = (b\$a)\S(c\$a)$.

Distributiviteten af $ med hensyn til § omtales i daglig tale som reglen om, at man kan "gange parenteser ud". Læg mærke til, at der er behov for både (17) og (18), fordi $ ikke behøver at være kommutativ.

Definition V.2. Hvis (A,§,$) er en organiseret mængde, hvori $ er distributiv med hensyn til §, siger man, at e er et ételement, hvis e er neutralt element ved $, altså hvis

(19) $\forall a \in A: a\$e = e\$a = a$

Af Sætning II.4 fremgår det, at der højst kan findes ét ételement i en mængde organiseret ved to kompositioner.

Definition V.3. Er (A,§,$) en mængde organiseret ved to kompositioner, kaldes den en ring, hvis (A,§) er en kommutativ gruppe, og hvis $ er en associativ komposition, der er distributiv med hensyn til §. Hvis $ tillige er kommutativ kaldes ringen for kommutativ.

I en ring kaldes § oftest "addition" og $ "multiplikation", selv om de ikke nødvendigvis refererer til de i talsystemerne opererende kompositioner. Som en naturlig følge heraf

man ofte + istedet for § og . i stedet for $, også i det almene tilfælde. Denne konvention vil vi også benytte her. Men vær opmærksom på, at der er tale om generelle kompositioner, hvilket betyder, at de kendte egenskaber fra + og · i talsystemerne ikke uden videre kan påberåbes.

Det bemærkes, at additionen i en ring altid er forudsat kommutativ. Det neutrale element ved addition kaldes også nulelementet og skrives O. Er der et ételement skrives dette sædvanligvis 1.

Sætning V.4. I en ring (A,+,·) gælder

(2o) $\forall a,b,c \in A: a\cdot(b - c) = (a\cdot b) - (a\cdot c)$

og

(21) $\forall a,b,c \in A: (b - c).a = (b.a) - (c\cdot a)$.

(Her angiver -x det inverse til x i forhold til additionen i ringen).

Bevis: Husk nu, at + og · angiver generelle kompositioner.

Vi har dels

$$a(b - c) + a(b + c) = a((b - c) + (b + c)) =$$
$$a(b - c + b + c) = a(b + b) = ab + ab$$

og dels

$$a(b - c) + a(b + c) = a(b - c) + ab + ac,$$

således at der ved sammenholdning fås

$$a(b - c) + ab + ac = ab + ab,$$

der medfører, at

$$a(b - c) = ab + ab - ab - ac = ab - ac,$$

hvilket skulle bevises.

Beviset for (21) forløber helt analogt.

Sætning V.5. Hvis (A,+,·) er en ring gælder

(22) $\forall a \in A: a\cdot O = O\cdot a = O$.

Bevis: Da $a\cdot O = a\cdot(O + O) = (a\cdot O) + (a\cdot O)$, hvor det første lighedstegn gælder, fordi O er neutralt element ved + og det andet på grund af distributiviteten, ses at

$$O = (a\cdot O) - (a\cdot O) = a\cdot O.$$

Tilsvarende ses, at $O\cdot a = O$, hvilket beviser sætningen.

På grund af dette forhold kan forkortningsreglerne ikke gælde for multiplikation i en ring, idet man altid har $a\cdot O = b\cdot O = O$ uden at a og b behøver at være identiske. Dette udtrykkes i daglige vendinger oftest sådan: "man kan ikke forkorte med O". Derimod kan man håbe på at kunne forkorte med alle andre faktorer end O: hvis $a\cdot c = b\cdot c$ er $a = b$, hvis $c \neq O$. Dette er i-

midlertid ikke muligt i enhver ring. Vi er interesseret i at studere ringe, hvori det er muligt. Vi formulerer reglen i en ændret skikkelse:

Definition V.6. I en ring siges nulreglen at gælde, hvis (i-det ringen hedder $(A,+,\cdot)$)

(23) $\quad \forall\, a,b\in A\colon a\cdot b = 0 \Rightarrow a = 0 \vee b = 0.$

At nulreglen er ækvivalent med reglen om forkortning med faktorer forskellige fra 0 fremgår af:

Sætning V.7. Nulreglen gælder i en ring, hvis og kun hvis

(24) $\quad \forall\, a,b\in A,\ c\in A\setminus\{0\}\ :\ a\cdot c = b\cdot c \Rightarrow a = b.$

Bevis: Lad os starte med at antage, at nulreglen gælder og lad $a,b\in A$, $c\in A\setminus\{0\}$ samt $a\cdot c = b\cdot c$. Så vil

$$0 = ac-bc = (a-b)\cdot c,$$

hvorfor $a - b = 0 \vee c = 0$. Da $c \neq 0$, må $a - b = 0$, altså $a = b$.

Hvis omvendt (24) gælder, kan vi vise nulreglen således:

Antag, at $a\cdot b = 0$. Vi skal vise, at $a = 0$ eller $b = 0$. Hvis dette var falsk, dvs. hvis både $a \neq 0$ og $b \neq 0$, måtte vi, da $a\cdot b = 0 = 0\cdot b$ og $b \neq 0$ have $a = 0$ i kraft af (24). Men dette er i strid med, at $a \neq 0$. Både a og b må således være forskellige fra 0, hvorved nulreglen er vist.

Definition V.7. En ring med ételement, hvori nulreglen gælder kaldes en integritetsring.

I ringe er der en række egenskaber ved multiplikationen, som ikke altid gælde, selv ikke hvis ringen er en integritetsring. I standardeksemplet på en integritetsring $(Z,+,\cdot)$, altså de hele tal forsynet med sædvanlig addition og multiplikation kan som bekendt ikke enhver division udføres. Vi ønsker at studere ringe, hvori (næsten) enhver division kan udføres. Som det fremgår af det foregående må division med 0 på forhånd undtages. Men alle andre divisioner ønsker vi at kunne udføre. At $(A,+,\cdot)$ er en ring, hvori dette kan lase sid gøre, er ensbetydende med, at $(A\setminus\{0\},\cdot)$ er en gruppe (kaldet den multiplikative gruppe). Vi definerer:

Definition V.8. Ved et legeme forstås en ring, hvor, idet ringen benævnes $(A,+,\cdot)$, $(A\setminus\{0\},\cdot)$ er en gruppe. Hvis multiplikationen er kommutativ taler vi om et kommutativt legeme.

Det fremgår, at ethvert legeme også er en integritetsring, idet nulreglen gælder, fordi multiplikationen er en gruppekomposition i $A\setminus\{0\}$, og idet denne gruppe har et ételement.

Vi må helle for en sikkerheds skyld formulere:

Sætning V.9 I et legeme har enhver ligning af formen

(25) $ax = b,\ a \neq 0$

og

(26) $xa = b,\ a \neq 0$

en entydigt bestemt løsning.
I et legemes multiplikative gruppe gælder forkortningsreglerne.

Bevis: Disse konklusioner er umiddelbart givet af forholdene i grupper (sætning II.11).

Lad os slutte med en definition vedrørende afbildninger mellem mængder med to eller flere kompositioner.

Definition V.10. Hvis $(A,\S_1,\ldots\S_n)$ og $(E,\$_1,\ldots\$_n)$ er mængder med hver n kompositioner og f afbilder A ind i E, siges f at være en homomorfi fra $(A,\S_1,\ldots\S_n)$ til $(E,\$_1,\ldots\$_n)$, hvis f er en homomorfi af hver $(A,\S_i)$ ind i $(E,\$_i)$ $(i=1,\ldots n)$. Tilsvarende kaldes f en isomorfi mellem $(A,\S_1,\ldots\S_n)$ og $(E,\$_1,\ldots\$_n)$, hvis f er en isomorfi mellem alle $(A,\S_i)$ og $(E,\$_i)$ $(i = 1,\ldots n)$.

Det ses, at en isomorfi også i dette almene tilgælde er en bijektiv homomorfi.

Det er nemt at indse, at isomorfier mellem organiserede mængder med flere kompositioner betyder, at de organiserede mængder har samme algebraiske struktur.

Liste over tidligere udsendte tekster kan rekvireres på IMFUFA's sekretariat, tlf. 4674 2263 eller e-mail: bs@ruc.dk

332/97 ANOMAL SWELLING AF LIPIDE DOBBELTLAG
Specialerapport af:
Stine Sofia Korremann
Vejleder: Dorthe Posselt

333/97 Biodiversity Matters
an extension of methods found in the literature on monetisation of biodiversity
by: Bernd Kuemmel

334/97 LIFE-CYCLE ANALYSIS OF THE TOTAL DANISH ENERGY SYSTEM
by: Bernd Kuemmel and Bent Sørensen

335/97 Dynamics of Amorphous Solids and Viscous Liquids
by: Jeppe C. Dyre

336/97 PROBLEM-ORIENTATED GROUP PROJECT WORK AT ROSKILDE UNIVERSITY
by: Kathrine Legge

337/97 Verdensbankens globale befolkningsprognose
- et projekt om matematisk modellering
af: Jørn Chr. Bendtsen, Kurt Jensen, Per Pauli Petersen
Vejleder: Jørgen Larsen

338/97 Kvantisering af nanolederes elektriske ledningsevne
Første modul fysikprojekt
af: Søren Dam, Esben Danielsen, Martin Niss, Esben Friis Pedersen, Frederik Resen Steenstrup
Vejleder: Tage Christensen

339/97 Defining Discipline
by: Wolfgang Coy

340/97 Prime ends revisited - a geometric point of view -
by: Carsten Lunde Petersen

341/97 Two chapters on the teaching, learning and assessment of geometry
by Mogens Niss

342/97 LONG-TERM SCENARIOS FOR GLOBAL ENERGY DEMAND AND SUPPLY
A global clean fossil scenario discussion paper
prepared by Bernd Kuemmel
Project leader: Bent Sørensen

343/97 IMPORT/EKSPORT-POLITIK SOM REDSKAB TIL OPTIMERET UDNYTTELSE AF EL PRODUCERET PÅ VE-ANLÆG
af: Peter Meibom, Torben Svendsen, Bent Sørensen

344/97 Puzzles and Siegel disks
by Carsten Lunde Petersen

345/98 Modeling the Arterial System with Reference to an Anestesia Simulator
Ph.D. Thesis
by: Mette Sofie Olufsen

346/98 Klyngedannelse i en hulkatode-forstøvningsproces
af: Sebastian Horst
Vejledere: Jørn Borggren, NBI, Niels Boye Olsen

347/98 Verificering af Matematiske Modeller
- en analyse af Den Danske Eulerske Model
af: Jonas Blomqvist, Tom Pedersen, Karen Timmermann, Lisbet Øhlenschlæger
Vejleder: Bernhelm Booss-Bavnbek

348/98 Case study of the environmental permission procedure and the environmental impact assessment for power plants in Denmark
by: Stefan Krüger Nielsen
Project leader: Bent Sørensen

349/98 Tre rapporter fra FAGMAT - et projekt om tal og faglig matematik i arbejdsmarkedsuddannelserne
af: Lena Lindenskov og Tine Wedege

350/98 OPGAVESAMLING - Bredde-Kursus i Fysik 1976 - 1998
Erstatter teksterne 3/78, 261/93 og 322/96

351/98 Aspects of the Nature and State of Research in Mathematics Education
by: Mogens Niss

352/98 The Herman-Swiatec Theorem with applications

by: Carsten Lunde Petersen

353/98 Problemløsning og modellering i en almendannende matematikundervisning

Specialerapport af: Per Gregersen og Tomas Højgaard Jensen

Vejleder: Morten Blomhøj

354/98 A GLOBAL RENEWABLE ENERGY SCENARIO

by: Bent Sørensen and Peter Meibom

355/98 Convergence of rational rays in parameter spaces

by: Carsten Lunde Petersen and Gustav Ryd

356/98 Terrænmodellering

Analyse af en matematisk model til konstruktion af terrænmodeller

Modelprojekt af: Thomas Frommelt, Hans Ravnkjær Larsen og Arnold Skimminge

Vejleder: Johnny Ottesen

357/98 Cayleys Problem

En historisk analyse af arbejdet med Cayley problem fra 1870 til 1918

Et matematisk videnskabsfagsprojekt af:

Rikke Degn, Bo Jakobsen, Bjarke K.W. Hansen, Jesper S. Hansen, Jesper Udesen, Peter C. Wulff

Vejleder: Jesper Larsen

358/98 Modeling of Feedback Mechanisms which Control the Heart Function in a View to an Implementation in Cardiovascular Models

Ph.D. Thesis by: Michael Danielsen

359/98 Long-Term Scenarios for Global Energy Demand and Supply Four Global Greenhouse Mitigation Scenarios

by: Bent Sørensen

360/98 SYMMETRI I FYSIK

En Meta-projektrapport af: Martin Niss, Bo Jakobsen & Tune Bjarke Bonné

Vejleder: Peder Voetmann Christiansen

361/99 Symplectic Functional Analysis and Spectral Invariants

by: Bernhelm Booss-Bavnbek, Kenro Furutani

362/98 Er matematik en naturvidenskab? - en udspænding af diskussionen

En videnskabsfagsprojekt-rapport af Martin Niss

Vejleder: Mogens Nørgaard Olesen

363/99 EMERGENCE AND DOWNWARD CAUSATION

by: Donald T. Campbell, MArk B. Bickhard and Peder V. Christiansen

364/99 Illustrationens kraft

Visuel formidling af fysik

Integreret speciale i fysik og kommunikation

af: Sebastian Horst

Vejledere: Karin Beyer, Søren Kjørup

365/99 To know - or not to know - mathematics, that is a question of context

by: Tine Wedege

366/99 LATEX FOR FORFATTERE

En introduktion til LATEX og IMFUFA-LATEX

af: Jørgen Larsen

367/99 Boundary Reduction of Spectral invariants and Unique Continuation Property

by Bernhelm Booss-Bavnbek

368/99 Kvartalsrapport for projektet
Scenarier for samlet udnyttelse af brint som energibærer i Danmarks fremtidige energisystem
Projektleder: Bent Sørensen
Opdateret til halvvejsrapport. Den nye udgave Tekst 368bis" kan hentes ned fra internettet fra adressen
http://mmf.ruc.dk/energy/report

369/99 Dynamics of Complex Quadratic Correspondences
by: Jacob Jalving

370/99 OPGAVESAMLING
Bredde-Kursus i Fysik 1976 – 1999
(erstatter tekst nr. 350/98)

371/99 Bevisets stilling -
beviser og bevisførelse i en gymnasial matematikundervisning
Matematikspeciale af: Maria Hermannsson
Vejleder: Mogens Niss

372/99 En kontekstualiseret matematikhistorisk analyse af ikke lineær programmering: Udviklingshistorie og multipel opdagelse
Ph.d.-afhandling af Tinne Hoff Kjeldsen

373/99 Criss-Cross Reduction of the Maslov Index and a Proof of the Yosida-Nicolaescu Theorem
by: Bernhelm Booss-Bavnbek, Kenro Furutani and Nobukazu Otsuki

374/99 Det hydrauliske spring
Et eksperimentelt studie af polygoner
Og hastighedsprofiler
Specialeafhandling af Anders Marcussen
Vejledere: Tomas Bohr, Clive Ellegaard og Bent C. Jørgensen

375/99 Begrundelser for Matematikundervisningen
i den lærde skole hhv. gymnasiet 1884-1914
Historie-speciale af: Henrik Andreassen

376/99 Universality of AC conduction in
disordered solids
by: Jeppe C. Dyre, Thomas B. Schrøder

377/99 The Kuhn-Tucker Theorem in
Nonlinear Programming:
A Multiple Discovery?
by: Tinne Hoff Kjeldsen

.....

378/00 Solar energy preprints:
Renewable energy sources and thermal energy storage
Integration of photovoltaic cells into the global
Energy system
by: Bent Sørensen

379/00 EULERS DIFFERENTIALREGNING
Eulers indførelse af differentialregningen stillet
over for den moderne
En tredjesemesters projektrapport på den
naturvidenskabelige basisuddannelse
af: Uffe Thomas Volmer Jankvist, Rie Rose Møller
Pedersen, Maja Bagge Petersen
Vejleder: Jørgen Larsen

380/00 Matematisk Modellering af Hjertefunktionen
Isovolumetrisk ventrikulær kontraktion og
udpumpning til det cardiovaskulære system
Speciale/3.moduls-rapport
af: Gitte Andersen, Jakob Hilmer, Stine Weisbjerg
Vejleder: Johnny Ottesen

381/00 Matematikviden og teknologiske kompetencer hos
kortuddannede voksne
- Rekognosceringer og konstruktioner i
grænselandet mellem matematikkens
didaktik og forskning i voksenuddannelse
Ph.d.-afhandling af Tine Wedege

382/00 Den selvundvigende vandring
Et matematisk professionsprojekt
af: Martin Niss, Arnold Skimminge
Vejledere: John Villumsen, Viggo Andreassen

383/00 Beviser i matematik
af: Anne K.S.Jensen, Gitte M.Jensen,
Jesper Thrane, Karen L.A.W.Wille,
Peter Wulff
Vejleder: Mogens Niss

384/00 Hopping in Disordered Media:
A Model Glass Former and A Hopping Model
Ph.d. thesis by Thomas B. Schrøder
Supervisor: Jeppe C. Dyre

385/00 The Geometry of Cauchy Data Spaces
by: Bernhelm Booss-Bavnbek, K. Furutani,
K.P. Wojciechowski